FAA BAA Call 3:
UAS Privacy Protections (005)

Contract Number: 697DCK-22-C-00265

Final Test Report (FTR)
Full Report with Appendices B & C

November 20, 2023

Document No.: TestReport-265_Honeywell_20231120-full-Rev2
Revision No.: 2.0

NOTICES

This material is provided to the US Federal Aviation Administration under Contract No. 697DCK-22-C-00265.

Export Classification: EAR 5E002.a

EXPORT CONTROLLED - This information is subject to the Export Administration Regulations (EAR) pursuant to 15 C.F.R. Parts 730-774. Transfer of this technology by any means to a non-U.S. Person, whether in the United States or abroad without the proper U.S. government authorization is strictly prohibited. Violations of the EAR may be subject to both criminal and administrative penalties under the Export Control reform Act of 2018 (50 U.S.C. §§ 4801-4852).

Prepared by:
Honeywell
Aerospace Advanced Technology, ACP RTC
Baltimore, MD, Redmond, WA and Minneapolis, MN

Northern Plains UAS Test Site
Grand Forks, ND

DOCUMENT REVISION LOG

Revision	Description	Date
1.0	Internal draft	27 Oct 2023
2.0	Added executive summary	20 Nov 2023

TRADEMARK DISCLAIMER

All product and company names used in this document are trademarks™ or registered® trademarks of their respective owners. Trademark symbols are included on the first instance of the product or company name and are implied for all other instances that do not include the trademark symbol.

Table of Contents

Table of Figures

List of Tables

FAA UAS PRIVACY PROTECTIONS (005) - EXECUTIVE SUMMARY

Introduction and Objectives:

The goal of this project was to mitigate cybersecurity risks and improve UAS security/privacy protections by leveraging industry-proven, high-maturity cybersecurity technologies and demonstrate the following key technology objectives:

- A scalable and interoperable security solution that uses industry-proven cybersecurity technology for the protection of information in transit and at rest.
- A multi-layered, defense-in-depth cybersecurity approach that includes RF link and end-to-end security to protect the confidentiality and integrity of information exchanges even when one layer of security is breached.
- Secure integration with commercial cloud services that segregate operator information in cloud-based storage, and which centralizes and facilitates secure multi-operator access to secure data storage with enforcement of data access only by the authorized operator.
- Effective sharing of the same commercial air/ground communication links (e.g., cellular, SATCOM) to carry both C2 application payloads (e.g., communicate, navigate, aviate, DAA) and user payload applications (e.g., imagery) while protecting the privacy, integrity, quality of service and segregation of each flow, for which the safety criticality may be different.

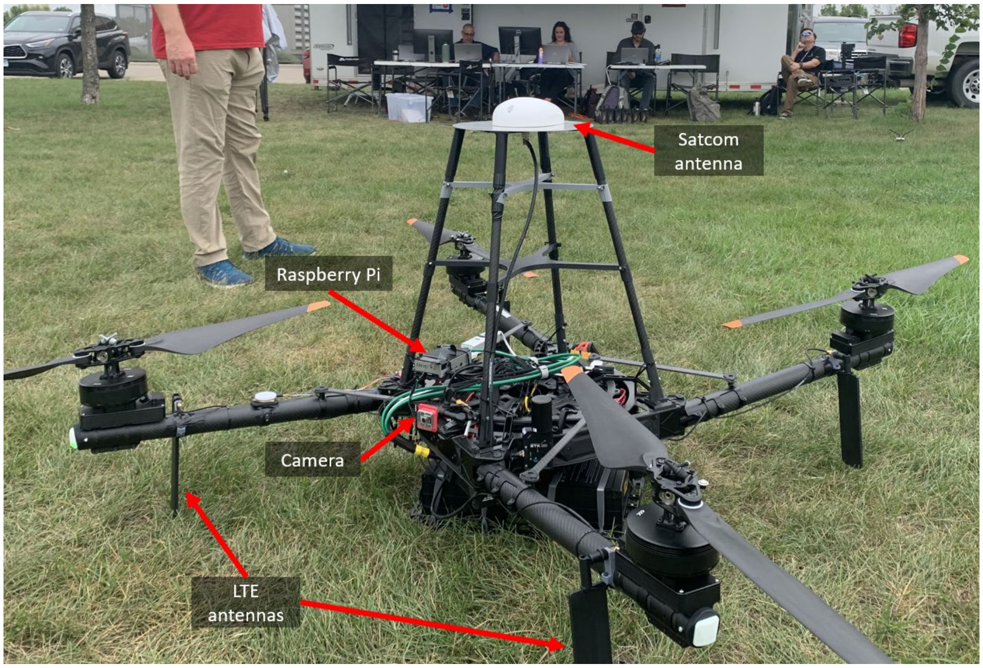
Previously, Honeywell successfully implemented and validated the RTCA DO-377A interworking and cybersecurity requirements in a laboratory environment and contributed to the refinement of those C2 MASPS requirements and associated means of compliance and addressed only the multi-link routing and security of the C2 link. This project built upon the prior work to address security/privacy of operator-sensitive payload information exchanged over shared commercial air/ground communication links and to mature the technology to TRL7 through a battery of flight tests, using representative applications and representative operational scenarios. Furthermore, commercial cloud-based data storage was integrated, which is an operator expectation for facilitating access to user application payload information from an UA operator.

Technology Description:

The multi-link UAS C2 communication system that was developed and demonstrated for this project used two commercially available radio links provided by a small-footprint SATCOM unit from Honeywell that contains both an Inmarsat SATCOM radio and a cellular/LTE radio. The SATCOM unit interfaced with a Raspberry Pi General Purpose Processor board, where the C2 link routing and security communication system was implemented. The C2 system was mounted and flown on a Freefly Alta-X drone. However, the Alta-X drone used an independent C2 link for vehicle control to mitigate the risk of depending on the C2 system under test for vehicle control and potentially losing vehicle control during the test flights.

The C2 Link System was controlled and monitored from the ground Control Station laptop by a ground-based CS Operator. The CS software and the Local Storage Management Application (LSMA) software run on the CS laptop, with internet connectivity through an LTE access point with access to the C2 Communication infrastructure (i.e., Satcom and LTE air-ground links to the UA) and to the Honeywell Cloud Service.

Our C2 system developed and used during this project had two levels of encryption and authentication over each of the links, first using endpoint encryption using WireGuard VPN, and second through the DTLS secure session between the DTSRs.



UAS C2 system installed on Alta-X drone for privacy protections demonstration.

Performance Results:

The system was evaluated on a total of 20 flights, plus 2 ground tests on the Alta-X drone. Six flights at each of 3 different inspection sites: a Water Tower Inspection, a linear power line inspection along a walking path trail, and a building; and 2 off-nominal flight tests at the building inspection site with DTLS encryption disabled.

Although the tests spanned multiple flights and multiple procedures, key metrics and parameters were collected consistently across all tests such as message latency, switchover times, and signal strength indicators for each of the links.

DO-377A specifies a latency requirement of 1.0 second at least 95% of the time. This latency requirement was met by both the SATCOM and the cellular/LTE links on all tests.

DO-377A MASPS specifies a requirement for RLP TET of under 3.0 sec. for surface, departure, arrival, and under 5.0 sec. for cruise in class B, C, E, & G airspaces. RLP TET was evaluated by the link switchover commands. During the testing for this project, a total of 68 manually commanded link switchovers were conducted. All 68 switchovers (100%) met the requirement and completed within the TET limit.

Findings and Lessons Learned

The objective of the UAS-PP project was to demonstrate a scalable security solution that uses industry-proven cybersecurity technology for the protection of information (in this case, images) that are transferred from a UAS to a ground control station and then made available to ground users via a commercial cloud storage service. All Key Performance Indicators (KPIs) and metrics for the UAS Privacy Protections Project were met at the conclusion of this project.

For this project, the team planned 11 inspections, two ground tests, 20 test flights, and System Security Verification (SSV) testing on the UAS-PP system. All inspections and tests were successfully performed. The tests and inspections largely passed, and in the cases of failures, the final report outlines why the failure occurred. The team advanced the TRL for the C2 system and the Honeywell VersaWave SATCOM system, improved the GFE software, and identified ways to advance the GFE software in future productization efforts. Improvements and weaknesses within the security framework in the UAS-PP are identified, should a future team seek to expand on this work. The UAS-PP tests and inspections successfully demonstrated that the security requirements from DO-377A can be implemented on a C2 system and applied to protect a user data stored on a commercial cloud service.

For next steps, Honeywell has considered how to progress the UAS work accomplished under this project and made submissions under Call 004 and Call 005 BAA that outline our recommended path forward in this area. In these whitepapers, Honeywell plans to incorporate the lessons learned from this project and flight test these improvements and additional features.

FAA UAS Privacy Protections (005)
Final Test Report

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to present the results of inspections, flight tests, and post-flight analyses performed for the Unmanned Aircraft System (UAS) Privacy Protections (UAS-PP) project under FAA Contract 697DCK-22-C-00265.

1.2 SCOPE

The scope of this report includes the qualitative and quantitative results of inspections and formal flight tests using a representative proof-of-concept system and procedure described in the Detailed Test Procedures [DTP] document.

The report summarizes the flight test results with respect to pass/fail criteria, provides post-test analysis results (e.g., quantitative time-based measurements), and reports the results of inspection activities performed interdependent of the flight tests. This document also presents lessons learned and recommendations for future tests/demonstrations.

1.3 DOCUMENT OVERVIEW

This document is organized into the following sections:

- Section 1 – Introduction

  This section identifies the purpose and scope of the document, summarizes the document organization and provides acronyms, definitions of terminology and references to applicable documents.

- Section 2 – System Under Test Configuration

  This section documents the final flight test configuration of the as-tested C2 Link System under test.

- Section 3 – Inspection and Test Summary

  This section summarizes the structure used in this document to present the result of inspection procedures and test procedures conducted on the C2 Link System under test.

- Section 4 – Inspection Results

  This section documents the detailed inspection and analysis procedures, including both project-specific procedures as well as procedures that are shared in common between the UAS Privacy Protections (UAS-PP) project and the UAS Command and Control (UAS-C2) project. Note that the common inspection/analysis procedures are repeated in each project-specific deliverable.

- Section 5 – Test Results

  This section presents the results of the formal flight and ground-based testing including: a summary of pass/fail results for each of the test cases performed; results of post-test analyses; and any variances or deviations encountered during testing.

- Section 6 – Summary and Recommendations

  This section provides an overall assessment of the test/inspection results, and where appropriate, provides lessons learned and recommendation for further testing.

- Appendix A – Expected Results

  This appendix documents the expected results for the verification steps in each test procedure.

- Appendix B – Inspection Results- UAS C2 Link System Security

  This appendix documents the results of the inspection for the link system security.

- Appendix C – Inspection Results- VPN for Protecting the UA to the CS

  This appendix documents the results of the inspection of the VPN.

- Appendix D – Technology Readiness Assessment

  This appendix documents the technology readiness assessment for the UAS-PP system.

- Appendix E – System Security Verification (SSV) Results

  This appendix documents the results of the SSV testing of the UAS-PP system.

1.4 TERMS AND ABBREVIATIONS

1.4.1 Acronyms

The following acronyms and abbreviations may appear in this document.

Acronym or Abbreviation	Definition
A/G	Air-Ground
AES	Advanced Encryption Standard
AGL	Above Ground Level
ANSI	American National Standards Institute
API	Application Programming Interface
ATC	Air Traffic Control
BAA	Broad Agency Announcement
C2	Command and Control
C2CSP	Command and Control Communication Service Provider
CM	Common
CS	Control Station
CSP	Communication Service Provider
DC	Direct Current
DSMA	Data Storage Management Application
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
DTP	Detailed Test Plan
DTSR	Data Transfer, Security and Routing
ECDHE	Elliptic Curve Diffie-Hellman - Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FAA	(US) Federal Aviation Administration
FIPS	Federal Information Processing Standards
FS	File System
FTP	Flight termination Point
GCM	Galois Counter Mode
GCS	Ground Control Station
GPS	Global Positioning System
GUI	Graphical user Interface
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transport Protocol – Secure
Hz	Hertz
ID	Identifier
IP	Internet Protocol
IP	Inspection Procedure
IPv4 / IPv6	Internet Protocol version 4 / version 6
IR	Interworking Requirement
ISM	Industrial, Scientific, and Medical
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LAANC	Low Altitude Authorization and Notification Capability
LMSF	Link Management and Security Function
LOS	Line of Sight
LSMA	Local Storage and Management Application
LTE	Long Term Evolution
LTS	Long Term Support
LZ	Landing Zone
MASPS	Minimum Aircraft System Performance Specification
MbB	Make-before-Break
MoC	Means of Communication
MP	Megapixel
MSG	Message
MTU	Maximum Transmission Unit
N/A	Not Applicable
NIST	National Institute of Standards and Technology

NPUASTS	Northern Plains UAS Test Site
NTP	Network Time protocol
OS	Operating System
PP	Privacy Protections
PPR	Privacy Protections Requirements
PR	Performance Requirement
RBAC	Role-Based Access Control
RF	Radio Frequency
RFC	Request For Comment
RLP	Required Link Performance
RLTP	Required Link Technical Performance
R-Pi	Raspberry Pi
RPIC	Remote Pilot In Command
Satcom	Satellite Communication
SER	Security Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SoW	Statement of Work
SR	Status Report
SRS	System Requirements Specification
SSL	Secure Sockets Layer
SSO	Single Sign-On
STP	System Test Plan
TC	Test Case
TCP	Transport Control Protocol
TP	Test Procedure
TET	Transaction Expiration Time
UA	Unmanned/Uncrewed Aircraft
UAS	Unmanned/Uncrewed Aircraft System
UAS-C2	UAS Command and Control (project)
UAS-PP	UAS Privacy Protections (project)
UDMD	User Data Multiplexer-Demultiplexer
UDP	User Datagram Protocol
UI	User Interface
UND	University of North Dakota
URL	Universal Resource Locator
US	United States
USB	Universal Serial Bus
VAC	Volts, Alternating Current
VDC	Volts, Direct Current
VLAN	Virtual Local Area Network
VLOS	Visual Line of Sight
VM	Virtual Machine
VPN	Virtual Private Network

1.4.2 Terminology

Term	Definition
C2 Link System	The totality of Air/Ground Links, Ground/Ground Links, and DTSR capabilities that support the exchange of C2 Link User Data between the CS and UA C2 Link Executive Management System.
C2 Link System Communication Service Provider	The C2 Link System Communication Service Provider (C2CSP) provides a portion of or all of the C2 Link System for the operation of a UAS. The C2CSP is integrated into the Safety Management System process of the certified UAS operation and is overseen by a Competent Authority designated by the certifying aviation authority.

Term	Definition
C2 Link System Control Messages	The various messages used to establish, maintain, terminate, switchover, and handover a C2 Link System Connection. These messages are carried on the logical Control Plane part of the C2 Link System Connection. Note: In this document, use of the truncated term "Control Messages" should be interpreted as "C2 Link System Control Messages."
C2 Link System Scheduled Switchover	A switchover that is scheduled to occur at a specific time and/or with the UA in a specific location.
C2 Link System User Data	Data coming from and going to CS and UA applications and subsystems that is exchanged over the C2 Link System Connection to support the remote pilot's Aviate, Communicate, Navigate, Integrate and Manage C2 Link System tasks. This data is carried on the logical User Plane part of the C2 Link System Connection. Note: In this document, use of the truncated term "User Data" should be interpreted as "C2 Link System User Data."
Control Messages	See definition for C2 Link System Control Messages
Control Plane Traffic	Control plane traffic is signaling traffic between CS and US C2 Link management functions to support establishing, maintaining, and terminating C2 Link System connectivity between the CS and UA. See definiton of C2 Link System Control Messages.
DTSR Subsystem	The subsystem that is responsible for establishing secure, i.e., authenticated, connections between per security systems on the UA and CS, for selecting the route/path that the C2 Link User Data flows and for switching the route when more than one path through the C2 Link is possible
Networked Link	A terrestrial or Satcom link between a UA and CS that uses a multiple access (multi-user) RF link between the UA and a Terrestrial or Satcom Air/Ground Access Network and a secure connection between the CS and the Air/Ground Access Network Gateway to provide a link between the UA and CS. This networked link may be provided by a C2 Link System Communications Service Provider (C2CSP).
User Data	See definition for C2 Link System User Data
User Plane Traffic	User plane (also called end-to-end or data plane) traffic is user traffic communicated between the UA and the pilot station. See definition of C2 Link System User Data.

1.5 APPLICABLE REFERENCE DOCUMENTS

The following documents are referenced in this report using the notation [XXX], where XXX is the shorthand document reference.

1.5.1 Industry – RTCA

Shorthand	Document Number	Document Description
DO-377A	DO-377A	Minimum Aviation System Performance Standards for C2 Link Systems Supporting Operations of Unmanned Aircraft Systems in US Airspace, 16 September 2021

1.5.2 Industry – NIST

Shorthand	Document Number	Document Description
38D	SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
56A	SP 800-56A, Rev. 3	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
131A	SP 800-131A, Rev. 2	Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019

Shorthand	Document Number	Document Description
		https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
180-4	FIPS 180-4	Secure Hash Standard (SHS), August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
186-4	FIPS 186-4	Digital Signature Standard (DSS), July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
197	FIPS 197	Advanced Encryption Standard (AES), November 2001 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
198-1	FIPS 198-1	The Keyed-Hashed Message Authentication Code (HMAC), July 2008 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

1.5.3 Industry – International Telecommunication Union (ITU)

Shorthand	Document Number	Document Description
X.509	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks, October 2019 https://www.itu.int/rec/T-REC-X.509-201910-I/en

1.5.4 Industry – Internet Request for Comment (RFC)

Shorthand	Document Number	Document Description
6347	RFC 6347	Datagram Transport Layer Security Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc6347

1.5.5 Project Documents

Shorthand	Document Number	Document Description
DTP	TestProcedures-265_HON_20230501	FAA BAA Call 3: UAS Privacy Protection (005) – Detailed Test Procedures, 01 May 2023
SRS	SRS-265_Honeywell_2020123	FAA BAA Call 3: UAS Privacy Protection (005) and UAS Command and Control (006) – System Requirements Specification, 23 January 2023
STP	TestPlan-265_HON_20230127	FAA BAA Call 3: UAS Privacy Protection (005) – System Test Plan, 27 January 2023

2 SYSTEM UNDER TEST CONFIGURATION

This section documents the final flight test configuration of the as-tested UAS-PP System under test.

2.1 FLIGHT TEST CONFIGURATION

2.1.1 Airborne System

The UAS-PP flight test configuration for the airborne system is illustrated in Figure 2-1. The C2 Link System interworking and security functionality is implemented in software running on a Raspberry Pi 4B computing platform (Figure 2-1, right). The integrated Honeywell VersaWave® Satcom and LTE radio avionics (Figure 2-1, upper-left) interconnects with the Raspberry Pi via an Ethernet connection using a USB-to-Ethernet converter. The Satcom and LTE radio avionics interface with a Satcom antenna unit and with four LTE antennas. Finally, a fixed mount Arducam 16MP camera (Figure 2-1, lower-left) interfaces with the Raspberry Pi via a ribbon cable that connects to a dedicated camera port provided on the Raspberry Pi.

The airborne components for the UA were integrated by NPUASTS on an Alta-X Freefly drone that was procured by NPUASTS. As part of the integration activity, NPUASTS provided an on-vehicle power module that supplies 28VDC to the Satcom+LTE avionics unit and 5VDC to the Raspberry Pi.

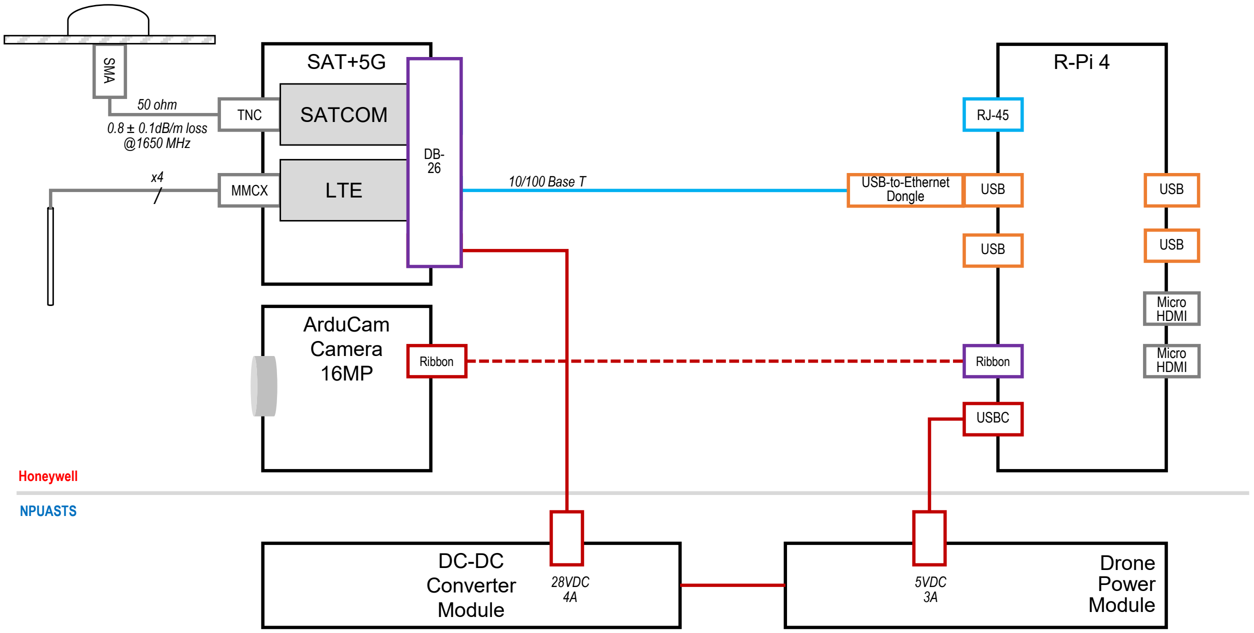


Figure 2-1. Airborne System Configuration for PP System on Alta-X drone

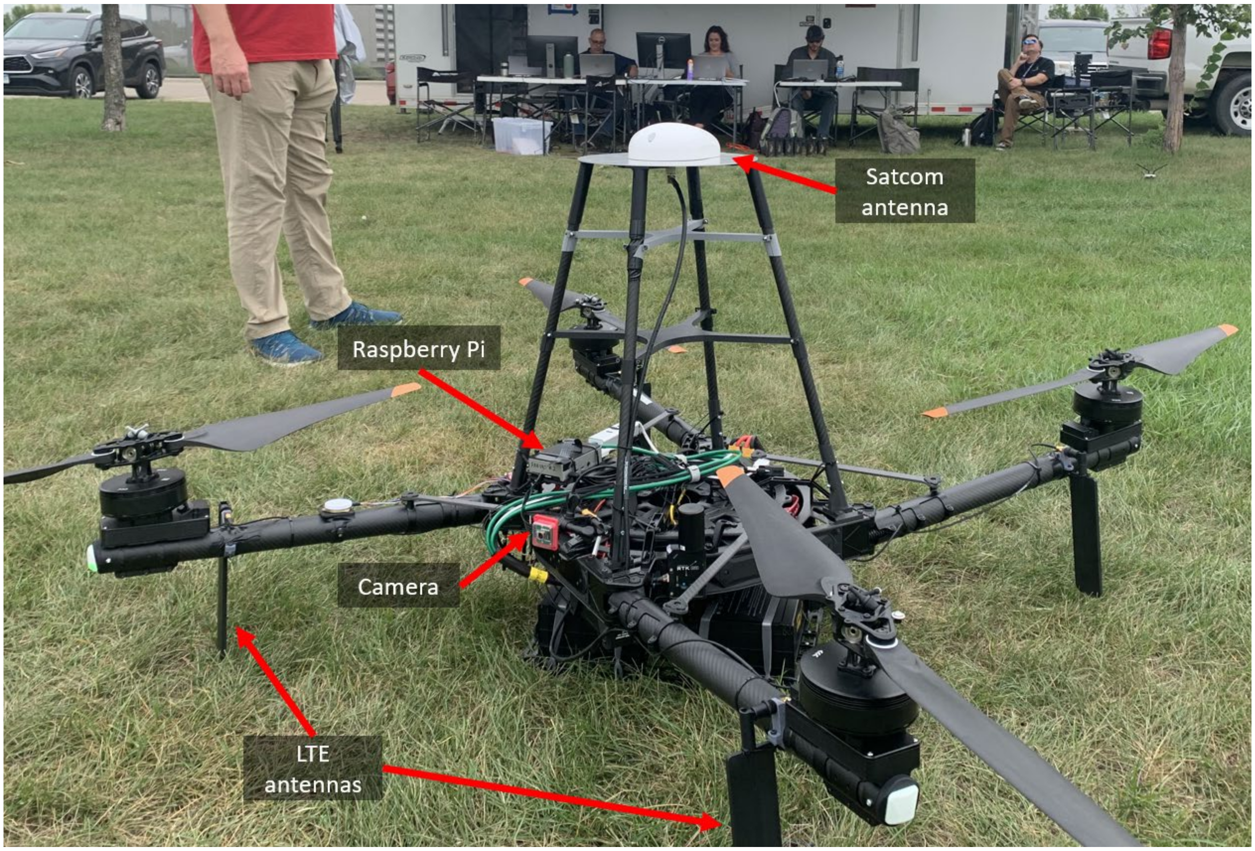


Figure 2-2. Alta-X drone Configured for PP System

2.1.2 Ground System

As illustrated in Figure 2-3, the C2 Link System was controlled and monitored from the ground Control Station laptop by a ground-based CS Operator. The CS laptop was installed in a NPUASTS mobile command center that provided internet connectivity via a CradlePoint IBR-900 ruggedized router provided by NPUASTS. The IBR-900 provides LTE connectivity to the internet, and it also includes a firewall, filtering, and threat management functionality.

The CS software and the Local Storage Management Application (LSMA) software run on two independent virtual machines using the VirtualBox hypervisor hosted on the CS laptop. The internet connectivity provides access to the C2 Communication Service Provider networking infrastructure (i.e., Satcom and LTE air-ground links to the UA) and to the Honeywell Cloud Service.

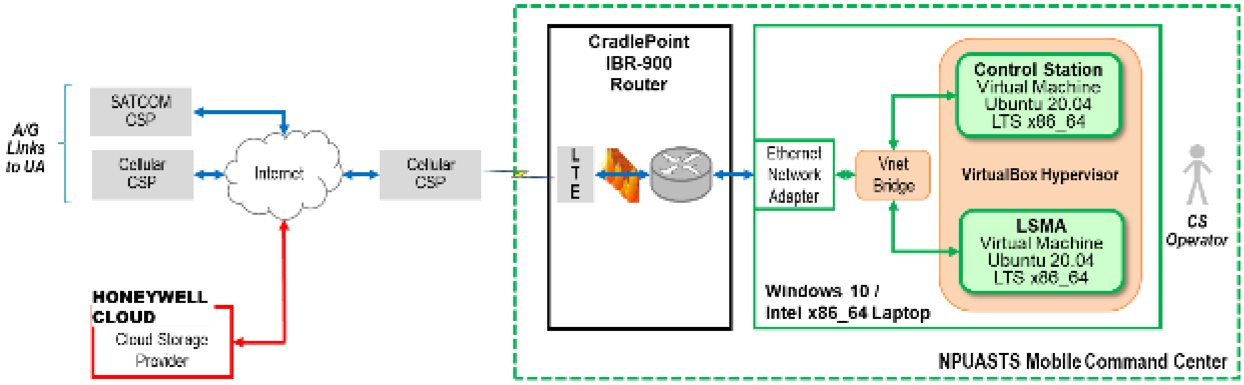

A/G Links to UA
SATCOM CSP
Cellular CSP
Internet
Cellular CSP
HONEYWELL CLOUD
Cloud Storage Provider
CradlePoint IBR-900 Router
LTE
Ethernet Network Adapter
Vnet Bridge
Control Station Virtual Machine Ubuntu 20.04 LTS x86_64
VirtualBox Hypervisor
LSMA Virtual Machine Ubuntu 20.04 LTS x86_64
Windows 10 / Intel x86_64 Laptop
CS Operator
NPUASTS Mobile Command Center

Figure 2-3. Ground System Configuration for PP System

2.2 FLIGHT TEST COMPONENT SUMMARY

The specific systems and components under test are documented in Table 2-1. The table includes a short description of the component, the model or part number, the serial number, and the software version (if applicable). Note that only key C2 Link System components are included; additional support systems (e.g., displays/monitors) and standard networking systems are not included.

Table 2-1 – SUT Component Summary

System	Component	Model/Part No.	Serial No.	Version	Comments
UA	HW: Drone	Freefly Alta-X Blue	AX363658	Package: 1.3.111 FMU: 1.3.31	Asset owned by NPUASTS QGroundControl: 1.3.9
UA C2 Link System Under Test	HW: Processor	Raspberry Pi 4B	e4:5f:01:05:42:9b	N/A	RPI #8
	HW: Ethernet Switch	Netgear ProSafe Plus GS105E	N/A	N/A	
	HW: SATCOM Radio	Honeywell Versawave Satcom+5G	11	N/A	Engineering Prototype
	HW: SATCOM Antenna	Honeywell 89000015-009	6108	N/A	Class15 Antenna
	HW: SATCOM RF Cable	Pasternack PE3W02802/HS-48	N/A	N/A	
	HW: SATCOM SIM	Honeywell 90411231	IMEI:89870-99204-15019-201	N/A	Inmarsat SBB via Honeywell Forge Connectivity
	HW: Cellular Antenna	Sierra Wireless 6001343	N/A	N/A	Qty = 4
	HW: Power Supply	Jackery Explorer 500	FU127080160448	N/A	Main battery bank
	HW: Power Supply	CUI VHK200W-Q48-S28	N/A	N/A	12VDC to 28VDC for Honeywell Satcom on Alta-X
	SW: Operating System	Raspberry Pi OS (64-bit) Linux	N/A	Bullseye 11 arm64 2023-05-03	Kernel: 5.15.61-v8+
	SW: UA C2 Link System Software	GFE	N/A	N/A	
	SW: Cryptographic Library	wolfSSL	N/A	4.4.0-gplv3-fips-ready	
	SW: Wireguard VPN	Wireguard	N/A	v1.0.20210223	
CS C2 Link System Under Test	HW: Router	CradlePoint IBR-1100	MM150120800336	7.0.40	Asset owned by NPUASTS (device aa1)
	HW: Processor	Dell Precision 7560	2NJB3M3	N/A	PC Name: MN74LT2NJB3M3
	SW: Operating System (Main)	Microsoft Windows 10 (x64)	N/A	Build: 19042.2846	Version: 20H2
	SW: Operating System (VM)	Ubuntu 20.04 (Focal) Linux	N/A	20.04.6 LTS x86_64	Kernel: 5.15.0-72-generic
	SW: Virtual Machine	VirtualBox Hypervisor	N/A	7.0.8 r156879	
	SW: CS C2 Link System Software	GFE	N/A	N/A	
	SW: Cryptographic Library	wolfSSL	N/A	4.4.0-gplv3-fips-ready	
	SW: Wireguard VPN	Wireguard	N/A	v1.0.20210223	

3 INSPECTION AND TEST REPORTING APPROACH

3.1 RESULT REPORTING

The inspection and test results reported in Sections 4 and 5 respectively are structured to present the following information:

- A summary-level result of the inspection or test using the values defined in Section 3.2. Where a test scenario consists of multiple test procedures, a summary-level result is included for each test procedure within the test scenario.
- Detailed results that are the output of an inspection procedure or a post-test analysis performed. For post-test analysis, the analysis output is compared with known

expected results, which are documented in Appendix A. If the analysis output matches the expected result, then no further detail if provided; however, in the event of a difference, and detailed explanation of the deviation is provided.

3.2 RESULT DEFINITIONS

The result of executing an inspection or test procedure may be one of the following:

Table 3-1 – Result Definitions

Result	Definition
PASS	The result complies with the Pass criteria specified in the detailed test procedures [DTP]
PARTIAL	The result complies partially with the Pass criteria specified in the detailed test procedures [DTP]. For example, positive results with an exception condition identified during the execution of one or more steps within a test procedure.
FAIL	The result does not comply with the Pass criteria (i.e., meets the Fail criteria) specified in the detailed test procedures [DTP].
NONE	An inspection or test procedure that could not be performed.

For any result other than "PASS," an explanation of any deviation/exception/issue is provided in the text as part of the detailed test result reporting.

4 INSPECTION RESULTS

This section documents the results of procedures where the requirement verification method is inspection or analysis, which are methods that were performed either prior to or after flight tests or ground-based tests.

4.1 RESULTS OF COMMON INSPECTION PROCEDURES

This section documents the result of inspection/analysis procedures that are shared in common between the UAS-PP and UAS-C2 projects. The inspection/analysis was performed once, but the results are reported in each project-specific final report deliverable.

4.1.1 IP_CM_001 – Crypto-Module Configuration

4.1.1.1 IP_CM_001A – UA AND CS C2 APPLICATION SOFTWARE CRYPTOGRAPHY

Result = PASS: This inspection shows that the system application software crypto-library is configured to use crypto-algorithms and key lengths that meet the requirements of NIST SP 800-131A, Rev2 (or equivalent MoC).

Detailed Results: Appendix B documents the detailed inspection results.

4.1.1.2 IP_CM_001B – VPN CRYPTOGRAPHY

Result = PARTIAL: This inspection shows that the VPN (Wireguard) is partially compliant with the security requirements in the MASPS. SER-02/SER-09, SER-03/SER-10, SER-04 and SER-11 pass. However, the key establishment scheme and security algorithms that Wireguard uses are only partially compliant.

Detailed Results:

Appendix C documents the detailed inspection results and further explains what parts of the security requirements are not fully MASPs compliant.

4.1.2 IP_CM_002 – User Data Performance during All Flight Phases

The logs containing User Data associated with each in-scope function (aviate, navigate) were analyzed to compute RLP Latency and RLP TET, and missing data duration.

- RLP Latency – The time for C2 Link User Data to pass, one-way, through the C2 Link System (i.e., UA DTSR, air/ground links, ground/ground links, CS DTSR) that was used to develop the TET.
- RLP TET – The maximum time that can be allowed for a transaction before airspace safety is materially affected.

Result = PASS: This inspection shows that for each airspace and operational condition, RLP Latency is less than the required time in that airspace. The time for 95% of User data messages to pass, one way, through the C2 link system meets the strictest limit of 1.0 sec. RLP TET was less than the TET limit for the cruise condition (5 seconds) for all commanded link switchovers.

Detailed Results:

For each flight, a stream of continuous user data was sent over the user data plane throughout the duration of the flight, both in the uplink and downlink directions. This data was representative C2 application data that was collected from a network capture of an actual flight of the Alta-X drone at NPUASTS. Messages were sent at a rate of 1 to 2 seconds, and each message varied in length between 50 and 600 bytes. Each message was analyzed and inspected to determine which link was used for its transmission and ensure its successful delivery at the receiver.

Latencies for each of these messages is defined as the elapsed time from when the message was sent to when the message was received by each of the DTSRs. However, due to the challenges from synchronizing both clocks from the sender and the receiver, our approach to latency analysis was to use the keep-alive messaging system, which measures the round-trip time of a message, subtracting the processing time by the remote receiver. These keep-alive messages were continuously sent throughout each flight over each link at a rate of about 1 message per second.

Some user data messages that were sent, failed a successful transmission and receipt by the receiver. The causes for failed message transmissions were during a link switchover, during a total link loss, or during times when the DTSR entered a failed state.

The latencies observed during our flights satisfy the strictest limit of 1.0 seconds for aviate and navigate messages on all airspaces and operational conditions. The average, median and percentage of user data traffic under 1 second latency are shown in Table 4-1. Section 5 shows the detailed data for each of the flights.

Table 4-1 – Link Latency per flight for 005-PP

Flight ID	Satcom Average Latency (ms)	Cellular Average Latency (ms)	SATCOM median latency (ms)	Cellular median latency	SATCOM % less than 1 sec	Cellular % less than 1 sec
Flight 1	605	199	535	196	100	100
Flight 2	582	202	527	200	100	100
Flight 3	605	197	535	195	100	100
Flight 4	618	197	530	194	99	100
Flight 5	591	197	527	194	100	100
Flight 6	586	201	523	198	99	100
Flight 7	576	203	524	199	99	100
Flight 8	630	195	562	191	98	100
Flight 9	594	190	534	187	99	100
Flight 10	582	190	527	186	99	100
Flight 11	570	189	523	186	100	100
Flight 12	582	195	521	191	98	100
Flight 13	574	200	525	197	100	100
Flight 14	600	189	534	187	99	100
Flight 15	577	197	529	194	100	100
Flight 16	576	200	523	193	100	100

Flight 17	586	194	539	191	100	100
Flight 18	638	195	601	191	97	100
Flight 19	631	196	598	190	99	100
Flight 20	582	192	539	188	100	100

Table 4-2 – User Plane Message delivery rate per flight for 005-PP

Flight ID	**User Messages Sent (uplink + downlink)**	**User Messages Received (uplink + downlink)**	**Success Rate (uplink + downlink)**
Flight 1	1,952	1,947	99.7%
Flight 2	1,330	648	48.7%
Flight 3	1,680	278	16.5%
Flight 4	1,298	1,295	99.8%
Flight 5	1,220	876	71.8%
Flight 6	1,060	1,057	99.7%
Flight 7	1,430	1,408	98.5%
Flight 8	1,674	501	29.9%
Flight 9	1,222	872	71.4%
Flight 10	1,335	1,331	99.7%
Flight 11	1,253	1,251	99.8%
Flight 12	1,093	1,090	99.7%
Flight 13	1,501	1,488	99.1%
Flight 14	1,345	1,343	99.9%
Flight 15	1,095	1,094	99.9%
Flight 16	1,100	1,093	99.4%
Flight 17	2,014	2,010	99.8%
Flight 18	2,115	2,112	99.9%
Flight 19	2,225	1,454	65.3%
Flight 20	2,074	2,071	99.9%
Total	**27,942**	**23,148**	**82.8%**

RLP TET was evaluated by the link switchover commands. Section 5.3 provides detailed results for each of the Switchover commands. In summary, out of the 68 switchovers, 100% completed the transaction within the TET limit of 5 seconds for the cruise operating condition.

4.2 PROJECT-SPECIFIC INSPECTION PROCEDURES

This section documents the results of inspection procedures that are specific to the UAS-PP project.

4.2.1 IP_PP_001 – Level of Preparedness Inspection Procedures

4.2.1.1 IP_PP_001A – UA C2 APPLICATION SOFTWARE AND OPERATING SYSTEM

Result = PASS: This inspection shows that the UA system application software is the latest tested version; and the operating system includes vendor-provided software/security patches/updates for the version installed on the computing platform (version that is accepted as industry best practice).

Detailed Results:

UA Application

Software change control for the C2 software was managed during development by using a hosted BitBucket repository application instance. BitBucket facilitates management and access to the software on a GIT software repository. The version of the C2 software that was finally released to conduct ground-based end-to-end tests was 2.0.1. Additional software changes, however, were needed to fix issues found during those tests. A BitBucket branch for each project was created based on software version 2.0.1 to keep track of those changes. The local software repository on the UA was updated from BitBucket with the appropriate project branch, and clean, build and configuration scripts were executed at the start of each test day to ensure the latest software version was being used.

The reported software version, however, does not include the name of the project branch. The version reported by the software was 2.0.1.

Operating System

- Output of *uname -a* command:

  ```
  Linux ua 6.1.21-v8+ #1642 SMP PREEMPT Mon Apr 3 17:24:16 BST 2023
  aarch64 GNU/Linux
  ```

- Contents of */etc/os-release* file:

  ```
  PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"

  NAME="Debian GNU/Linux"

  VERSION_ID="11"

  VERSION="11 (bullseye)"

  VERSION_CODENAME=bullseye

  ID=debian

  HOME_URL="https://www.debian.org/"

  SUPPORT_URL="https://www.debian.org/support"

  BUG_REPORT_URL=https://bugs.debian.org/
  ```

4.2.1.2 IP_PP_001B – CS C2 APPLICATION SOFTWARE AND OPERATING SYSTEM

Result = PASS: This inspection shows that the CS system application software is the latest tested version; the operating system includes vendor-provided software/security patches/updates for the version installed on the computing platform (version that is accepted as industry best practice); anti-virus software includes vendor-provided software/security patches/updates and latest vulnerability signature files, and no threats are identified during a full scan.

Detailed Results:

CS Application

The version reported by the software was 2.0.1. That is the correct version for conducting ground-based end-to-end tests.

Operating System

- Output of *uname -a* command:

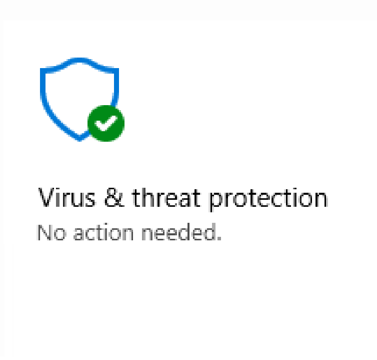
```
    Linux cs 5.15.0-83-generic #92~20.04.1-Ubuntu SMP Mon Aug 21 14:00:49
UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

- Contents of */etc/os-release* file:

```
    NAME="Ubuntu"
    VERSION="20.04.6 LTS (Focal Fossa)"
    ID=ubuntu
    ID_LIKE=debian
    PRETTY_NAME="Ubuntu 20.04.6 LTS"
    VERSION_ID="20.04"
    HOME_URL="https://www.ubuntu.com/"
    SUPPORT_URL="https://help.ubuntu.com/"
    BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
    PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-
policies/privacy-policy"
    VERSION_CODENAME=focal
    UBUNTU_CODENAME=focal
```

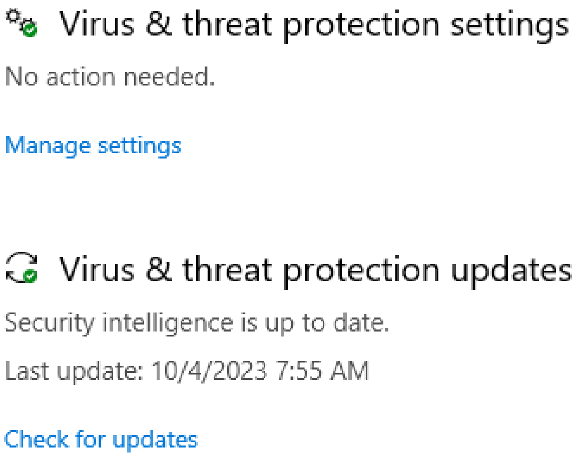
Anti-virus

Anti-virus software is provided by Microsoft Defender from the Windows Operating System. The system was checked, and it was verified to be active, current, and up-to-date.



Virus & threat protection

No action needed.



Virus & threat protection settings

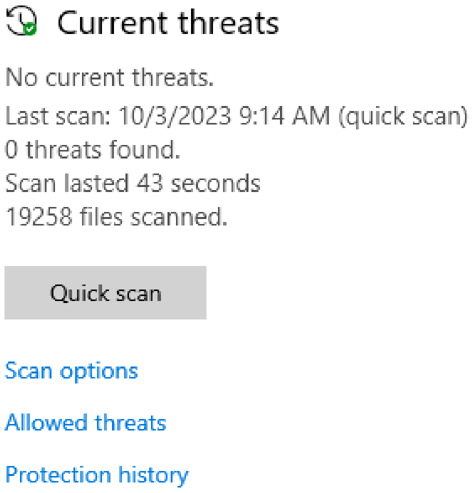
No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Last update: 10/4/2023 7:55 AM

Results of system scan showing that no threats were identified.



Current threats

No current threats.
Last scan: 10/3/2023 9:14 AM (quick scan)
0 threats found.
Scan lasted 43 seconds
19258 files scanned.

4.2.1.3 IP_PP_001C – LOCAL STORAGE APPLICATION AND OPERATING SYSTEM

Result = PASS: This inspection shows that the LSMA system application software is the latest tested version; the operating system includes vendor-provided software/security patches/updates for the version installed on the computing platform (version that is accepted as industry best practice); anti-virus software (if installed) includes vendor-provided software/security patches/updates and latest vulnerability signature files, and no threats are identified during a full scan.

Detailed Results:

LSMA Client Version

LSMA software module	Bitbucket branch name	Bitbucket tag name

FAA-UAS-WEB/FAA-UAS-CLIENT	master	1.0.0

Operating System

- Output of *uname -a* command:

```
Linux lsma 5.15.0-79-generic #86~20.04.2-Ubuntu SMP Mon Jul 17 23:27:17 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

- Contents of */etc/os-release* file:

```
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.6 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

4.2.1.4 IP_PP_001B – CLOUD STORAGE APPLICATION AND OPERATING SYSTEM

Result = PASS: This inspection shows that the DSMA system application software is the latest tested version; the operating system includes vendor-provided software/security patches/updates for the version installed on the computing platform (version that is accepted as industry best practice).

Detailed Results:

DSMA Application

DSMA software module versions

DSMA software module	Bitbucket branch name	Build version in Octopus (used for deployment to AKS)	Deployed version in AKS app hosting cluster
FAA-UAS-DSMA-faa-uas-dsma-xAPI	init	0.1.2-init0003	0.1.2-init0003
FAA-UAS-DSMA-faa-uas-dsma-sAPI	init	0.1.2-init0055	0.1.2-init0055
FAA-UAS-IAM-policy-agent	init	0.1.1-init0015	0.1.1-init0015

FAA-UAS-IAM-rbac	init	0.1.1-init0015	0.1.1-init0015

Evidence of deployed software versions:

Octopus Release Notes:

FAA-UAS-DSMA-faa-uas-dsma-xAPI:

Version: 0.1.2-init0003 commit babde31824a8a34e30abbd6a8f8135ad962f9a44 Author: GLOBAL\E159786 rajeev.mohan@honeywell.com Date: Fri Jul 28 20:22:17 2023 +0530

FAA-UAS-DSMA-faa-uas-dsma-sAPI:

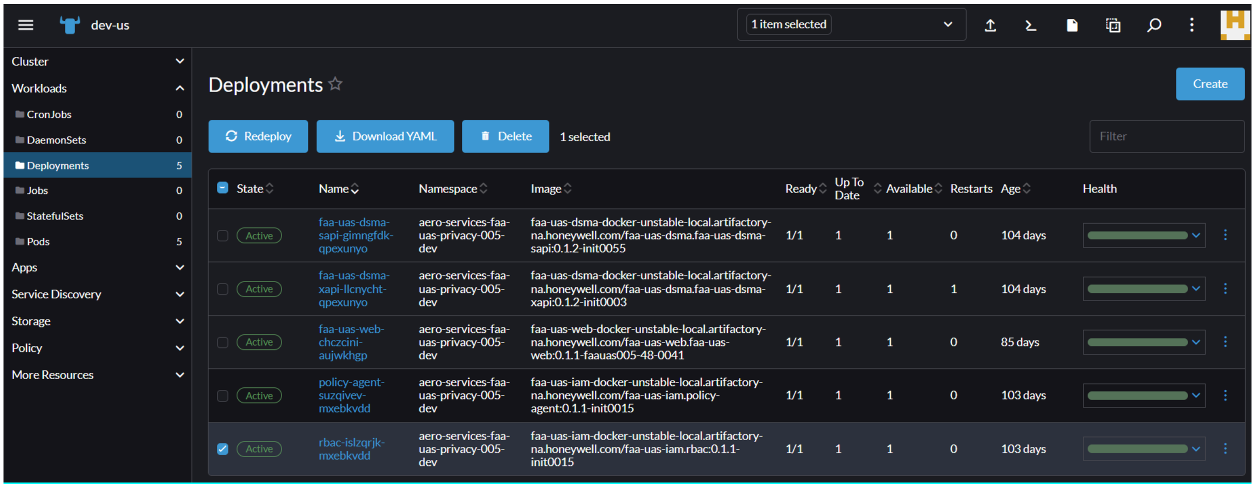
Version: 0.1.2-init0055 commit 2fcfdd440fd3e300c6856e54297810adb26030ae Author: GLOBAL\E159786 rajeev.mohan@honeywell.com Date: Thu Jul 27 22:07:42 2023 +0530

FAA-UAS-IAM-policy-agent:

Version: 0.1.1-init0015 commit a23e6524b741ff88588855361fe3aa013f6bcd69 Author: GLOBAL\E159786 rajeev.mohan@honeywell.com

FAA-UAS-IAM-rbac:

Version: 0.1.1-init0015 commit 3e5407de33cff09dc26ccadae5e5f855a43f8e76 Author: GLOBAL\E159786 rajeev.mohan@honeywell.com



State	Name	Namespace	Image	Ready	Up To Date	Available	Restarts	Age	Health
□ Active	faa-uas-dsma-sapi-gimngfdk-qpexunyo	aero-services-faa-uas-privacy-005-dev	faa-uas-dsma-docker-unstable-local.artifactory-na.honeywell.com/faa-uas-dsma.faa-uas-dsma-sapi:0.1.2-init0055	1/1	1	1	0	104 days	🟩
□ Active	faa-uas-dsma-xapi-llcnycht-qpexunyo	aero-services-faa-uas-privacy-005-dev	faa-uas-dsma-docker-unstable-local.artifactory-na.honeywell.com/faa-uas-dsma.faa-uas-dsma-xapi:0.1.2-init0003	1/1	1	1	1	104 days	🟩
□ Active	faa-uas-web-chczcini-aujwkhgp	aero-services-faa-uas-privacy-005-dev	faa-uas-web-docker-unstable-local.artifactory-na.honeywell.com/faa-uas-web.faa-uas-web:0.1.1-faauas005-48-0041	1/1	1	1	0	85 days	🟩
□ Active	policy-agent-suzqivev-mxebkvdd	aero-services-faa-uas-privacy-005-dev	faa-uas-iam-docker-unstable-local.artifactory-na.honeywell.com/faa-uas-iam.policy-agent:0.1.1-init0015	1/1	1	1	0	103 days	🟩
☑ Active	rbac-islzqrjk-mxebkvdd	aero-services-faa-uas-privacy-005-dev	faa-uas-iam-docker-unstable-local.artifactory-na.honeywell.com/faa-uas-iam.rbac:0.1.1-init0015	1/1	1	1	0	103 days	🟩

Figure 4-1 Deployed Cloud Application Software Versions

Figure 4-1 shows the version numbers for the DSMA software used to conduct ground-based end-to-end tests.

Operating System

Azure Kubernetes Services (AKS) Version: v1.25.11

Details on Kubernetes version: https://kubernetes.io/blog/2022/08/23/kubernetes-v1-25-release/

AKS uses Windows Server 2019 and Windows Server 2022 as the host OS version. As part of SLA, Microsoft assures the resources get the latest patches.

4.2.2 IP_PP_002 – User Data Isolation

4.2.2.1 IP_PP_002A – LOCAL STORAGE USER DATA ISOLATION

Result = PASS: This inspection shows that the local storage solution provides logical isolation of User Data using cryptographic algorithms and keys that comply with the MoC for SER-01 through SER-05.

Detailed Results:

The LSMA is implemented by an Ubuntu virtual machine, hosted on the CS laptop. The CS Operator transfers user content from the UA to the LSMA by executing scripts that use two individual openSSH *secure copy* (`scp`) commands; one command to copy the content from the UA to the CS, and another command to copy it from the CS to the LSMA. Both invocations of the scp command are done from the CS OS terminal and with the default cipher. The CS Operator is authenticated by the UA and the LSMA using asymmetric key cryptography. An asymmetric RSA key pair of length 4096 was created on the CS prior to the ground tests. The corresponding public key was installed on the UA and the LSMA as authorized keys for the CS Operator user (`uas-user`).

Public key for user `uas-user` on CS:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDGg3m6W4BSeCaVfy37d0QclMkXUUgwq9M3sxCYGweMk8Z1D
6g9P3a69WcYgmHu7zwmxgQ8gwQMWx+5pyFCagTrBAQjEGa8eTFdRg9y4+XHfuc7mGNkhbdjKN3Cbh
2JZPUBiNpyiu1MpY8PF/WX3Dto3eydC2AMjbhDHy8jWTKN3xLdp/4pXozK8GT33eTVIhjEPydGudq
+hn+KKEl4YmsMjyxhsxbNaytR8oJ8ke/MsSv5VwoSQR4tqZ1UDhXyPhIyJZI4XujhDAAD7CEnFitp
l5VCM4N1BjfGpZo0U/GvktrPo1jr1r519W3oJmCH9EMnXH1/6Xy0ii67navD4qafVvpXq4nBE/KmS
a6BBbD4MKa0xw8yuz55Blmeh729QDIEAnQNjci5ptTC/kVauFzLy2Kgi1ujFWgUZpAupDaJLmQG6O
fb/drnk6s8vM3eFNTgeoz3PUBW8c2iGxanKl3ciSQ769JnZ1n79yuqTfQTi/XEOPJpmLQE8ZAx/hV
S2HN49T+oU3izYLeeAyXjPQTBYSt0AYb5Rc6AiULQR2QVyekC2QkH4hdwj6PsBB6CasdaY1ZO2j/O
beVyC/RfMeazPwwWY1rsMFAn1cNXbFbNeLNKx1ewEOhg+3higgLcxn7bEUHjj3y60O2m+2GAY4Cn8
oRLBjZEooGG/jMLHWlnuQ== uas-user@gcs
```

Contents of the authorized_keys file on the LSMA:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDGg3m6W4BSeCaVfy37d0QclMkXUUgwq9M3sxCYGweMk8Z1D
6g9P3a69WcYgmHu7zwmxgQ8gwQMWx+5pyFCagTrBAQjEGa8eTFdRg9y4+XHfuc7mGNkhbdjKN3Cbh
2JZPUBiNpyiu1MpY8PF/WX3Dto3eydC2AMjbhDHy8jWTKN3xLdp/4pXozK8GT33eTVIhjEPydGudq
+hn+KKEl4YmsMjyxhsxbNaytR8oJ8ke/MsSv5VwoSQR4tqZ1UDhXyPhIyJZI4XujhDAAD7CEnFitp
l5VCM4N1BjfGpZo0U/GvktrPo1jr1r519W3oJmCH9EMnXH1/6Xy0ii67navD4qafVvpXq4nBE/KmS
a6BBbD4MKa0xw8yuz55Blmeh729QDIEAnQNjci5ptTC/kVauFzLy2Kgi1ujFWgUZpAupDaJLmQG6O
fb/drnk6s8vM3eFNTgeoz3PUBW8c2iGxanKl3ciSQ769JnZ1n79yuqTfQTi/XEOPJpmLQE8ZAx/hV
S2HN49T+oU3izYLeeAyXjPQTBYSt0AYb5Rc6AiULQR2QVyekC2QkH4hdwj6PsBB6CasdaY1ZO2j/O
beVyC/RfMeazPwwWY1rsMFAn1cNXbFbNeLNKx1ewEOhg+3higgLcxn7bEUHjj3y60O2m+2GAY4Cn8
oRLBjZEooGG/jMLHWlnuQ== uas-user@gcs
```

SSH server cryptographic configuration on the LSMA:

```
gssapikexalgorithms gss-gex-sha1-,gss-group14-sha1-

ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-
ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-
64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

```
kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-
hellman-group14-sha256
```

4.2.2.2 IP_PP_002B – CLOUD STORAGE USER DATA ISOLATION

Result = PASS: This inspection shows that the cloud storage solution provides logical isolation of User Data using cryptographic algorithms and keys that comply with the MoC for SER-01 through SER-05.

Detailed Results:

PPR-03:

- LSMA invokes DSMA APIs using JWT generated from Honeywell CWA through a Client Id/Client secret pair
- LSMA uses Client Id registered in Honeywell CWA: Client_zqaza137zcq7
- The generated token is checked by the Cloud RBAC applications (**FAA-UAS-IAM-policy-agent and FAA-UAS-IAM-rbac)** for authorization to invoke the APIs.
- Verified that the following APIs are invoked by LSMA using the Client Id/Secret pair:
- https://xapi-dev.uas005.qaero.honeywell.com/api/v1/files/upload/<activityId>
- https://xapi-dev.uas005.qaero.honeywell.com/api/v1/files/uploadComplete/<activityId>
- where the organization identity is provided as part of header field <**organization**> where organization is either ORG-A/ORG-B/ORG-C

PPR-04:

- Verified that the files uploaded for each customer is stored within the container allocated for the user.
- Uploaded Org A encrypted files are stored in storage account uasprivacy005sadev under container org-a with folder path: /raw-data/{activityId}/{imageFileName}
- Uploaded Org B encrypted files are stored in storage account uasprivacy005sadev under container org-b with folder path: /raw-data/{activityId}/{imageFileName}
- Uploaded Org C encrypted files are stored in storage account uasprivacy005sadev under container org-c with folder path: /raw-data/{activityId}/{imageFileName}
- After decrypting the uploaded files using the asymmetric key pair (RSA algorithm) where private key is specific to the organization as well as the symmetric key (AES algorithm) the files are stored in the container with folder name: /processed-data/{activityId}/{imageFileName}

Encryption by Azure platform: All the files stored in Azure data storage are encrypted as every Azure Storage account has encryption enabled by default, and it cannot be disabled. SSE transparently encrypts the data when writing to Azure storage and decrypts the data before it is read. The encryption uses 256-bit AES encryption which is one of the strongest block ciphers available. SSE uses encryption keys managed by Microsoft in which case, Microsoft generates the keys and handles their secure storage along with rotating the keys regularly on a schedule known only to Microsoft.

PPR-05:

LSMA invokes the DSMA API to upload encrypted image files along with IV and cypher files to allow for decryption of the image files in the DSMA.

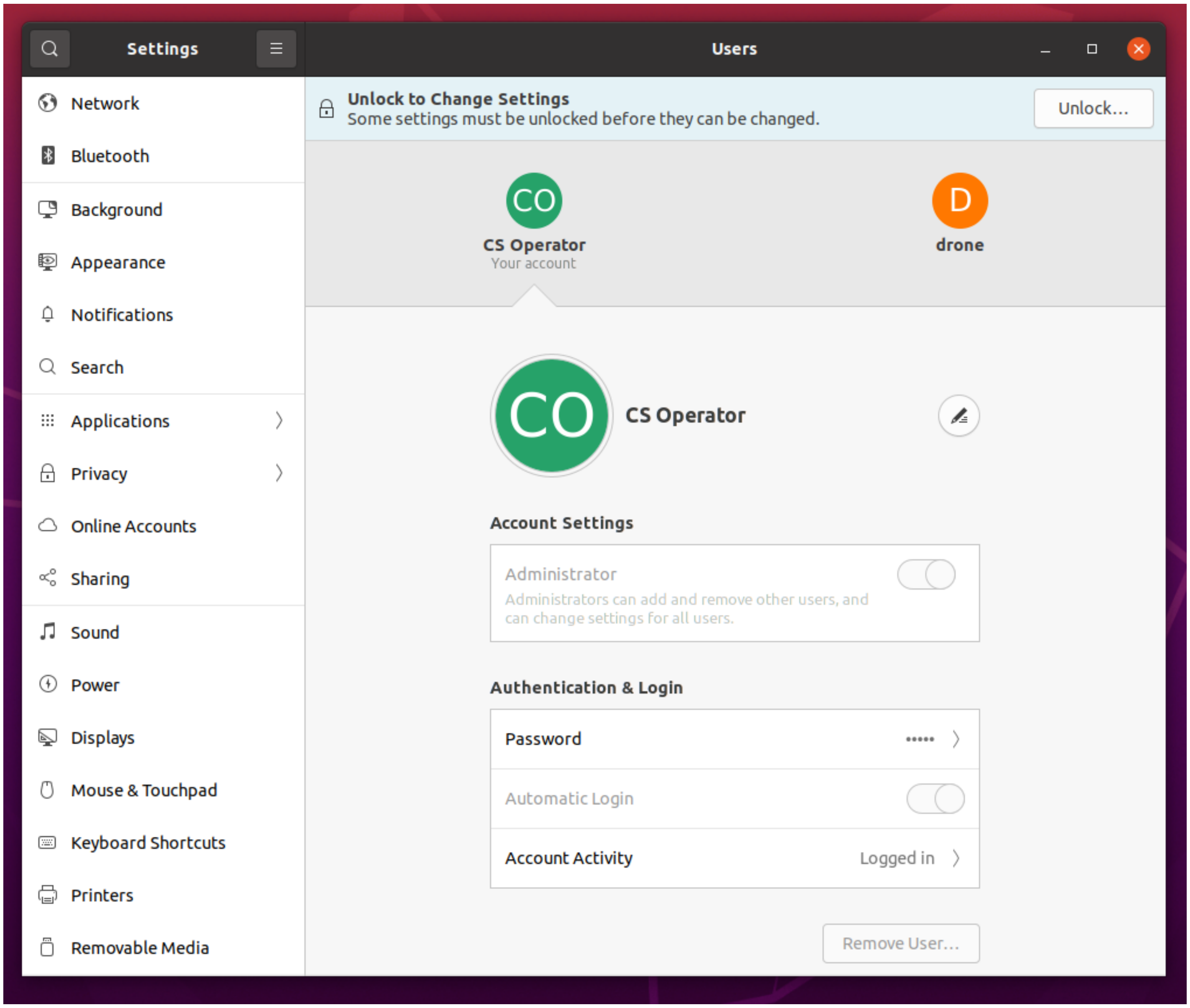
4.2.3 IP_PP_003 – Access Management

4.2.3.1 IP_PP_003A – LOCAL STORAGE LEAST PRIVILEGE

Result = PASS: This inspection shows that the local storage solution provides role-based access control and limits administrative access to select users.

Detailed Results:

Figure 4-2 shows the user management application provided by the Ubuntu operating system. It provides a means for assigning or revoking system access privileges. Note that only a subset of users have administrator privileges.



Unlock to Change Settings
Some settings must be unlocked before they can be changed.

CS Operator
Your account

drone

CS Operator

Account Settings

Administrator
Administrators can add and remove other users, and can change settings for all users.

Authentication & Login

Password •••••

Automatic Login

Account Activity Logged in

Figure 4-2 LSMA Role-based Access and Least Privilege

The Ubuntu operating system of the LSMA provides role-based user access control and limits administrative access to select users. Figure 4-2 shows a view of the user management application provided by Ubuntu. It shows the existing users on the LSMA and application controls that can be used to grant or refuse administrative access to selected users.

4.2.3.2 IP_PP_003B – CLOUD STORAGE LEAST PRIVILEGE

Result = PASS: This inspection shows that the cloud storage solution provides role-based access control and limits administrative access to select users.

Detailed Results:

Table 4-1 shows a complete list of users for each role defined for cloud application software. Only a reduced subset of users have administrator privileges. Each role has only the required permissions to perform its associated functions. In particular, only users in a particular organization (e.g. A, B or C) have permissions to access resources private to that organization. The CS Operator user can only download dispatch files and upload content for activities associated with any organization. On a production environment, there would be no users active with a developer role.

Role	Access to Resources	Permission Details	User List
Honeywell FAA UAS 005 Admin	"resources": ["uas005/files/encrypted/**", "uas005/files/decrypted/**", "uas005/activity/**", "uas005/dispatch/**", "uas005/keys/**"]	"permissions": ["uas005.keymanagement.*", "uas005.dispatch.*", "uas005.activity.*", "uas005.encrypted.upload", "uas005.encrypted.read", "uas005.decrypted.read"] Admin users can perform the following activities: - Upload Files to Cloud - View all files stored in cloud storage - Create or Delete an activity for all organizations - Create or Delete a dispatch plan for all organizations - Create/Delete/Read RSA key pair for each organization (public/private keys) for all organizations	1. e159786: Rajeev Mohan (Software architect) 2. e019570: Mike Olive (EID disabled after retirement) 3. h527677: John Cole (Cyber security) 4. h406457: Daniel Quiroz (Cyber security) 5. h505421 :Suzanne Hawkins (Program Mgr)
FAA UAS 005 Organization A user	"resources": ["uas005/files/decrypted/org-a","uas005/activity/org-a",	"permissions": ["uas005.keymanagement.read", "uas005.dispatch.*", "uas005.activity.*", "uas005.decrypted.read"	User: 3188818849163f62 (email id: faa_uas0a@aol.com)

	"uas005/dispatch/org-a"]],	] Organization A user who has following access: - View decrypted files in Cloud for Organization A - create/delete an Activity for Organization A - create/delete a dispatch for Organization A - Read public key for Organization A	
FAA UAS 005 Organization B user	"resources": ["uas005/files/decrypted/org-b","uas005/activity/org-b","uas005/dispatch/org-b"]	"permissions": ["uas005.keymanagement.read", "uas005.dispatch.*", "uas005.activity.*", "uas005.decrypted.read"] Organization B user who has following access: - View decrypted files in Cloud for Organization B - create/delete an Activity for Organization B - create/delete a dispatch for Organization B - Read public key for Organization B	1. e517781 (Pedro Davalos – Program manager) **2.** 225751886d145aac (email id :faa_uas0b@aol.com)
FAA UAS 005 Organization C user	"resources": ["uas005/files/decrypted/org-c","uas005/activity/org-c","uas005/dispatch/org-c"]	"permissions": ["uas005.keymanagement.read", "uas005.dispatch.*", "uas005.activity.*", "uas005.decrypted.read"] Organization C user who has following access: - View decrypted files in Cloud for Organization C - create/delete an Activity for Organization C create/delete a dispatch for Organization C	1. e159713: Mohan Tomar (Cloud S/W Mgr) 2. 902581886d16bed6 (email id: faa_uas0c@aol.com)
Honeywell FAA UAS 005 Developer	"resources": ["uas005/files/encrypted/**", "uas005/files/decrypted/**",	"permissions": ["uas005.keymanagement.read", "uas005.dispatch.*", "uas005.activity.*",	h293178: Matthew Tarbutton (Cloud Developer)

	"uas005/activity/**", "uas005/dispatch/**", "uas005/keys/**"]	"uas005.decrypted.read", "uas005.encrypted.read"] Honeywell Developer who has access to the following resources: - View encrypted files in Cloud storage for all organizations. - View decrypted files in Cloud storage for all organizations. - Create/Delete activity for all organizations - Create delete Dispatch for all organizations - Create/Delete/Read RSA key pair for all organizations	
FAA UAS 005 CS Operator	"resources": ["uas005/files/encrypted/**", "uas005/activity/**", "uas005/dispatch/**"]	"permissions": ["uas005.keymanagement.read", "uas005.dispatch.read", "uas005.activity.read", "uas005.encrypted.upload"] Drone operator who has the following permissions: - Read public key of RSA key pair - Read Dispatch plan for every organization - Read Activity of every organization - Upload encrypted file to cloud storage	Users: h510010 (Carlos Velez)

Table 4-3 Users Access Permissions for Application Software

5 TEST RESULTS

This section documents the results of test procedures where the requirement verification method is test or demonstration, which are methods that were performed during flight tests or ground-based tests.

5.1 FLIGHT TEST RESULTS

This section documents the results of flight test performed in accordance with flight test cards and detailed test procedures specified in [DTP]. Each flight test identifies the associated test card and test scenario, the flight number (within the series of twenty flight tests), the test date, and the test start/end times. General test observations (e.g., issues or unexpected conditions encountered during the flight test) are documented. The test results, which are presented in a tabular form, identity the individual test procedures specified in the test card, report the result of each test procedure, and provide notes, as necessary, to describe conditions observed during the execution of the specific test procedure and/or to explain a result other than pass.

5.1.1 Target A – Water Tower – Flight 1-of-6 (Nominal)

Result = PARTIAL: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET. However, several test procedures in the sequence failed after encountering a software error.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	1	24 Aug 2023	11:52 CDT	12:19 CDT

General Test Observations: The UA and CS DTSRs got out of sync twice during this flight; first this issue caused TP_CM004A to fail. The testers restarted the DTSRs to reset the systems and the system recovered for a while. However, later the same issue caused TP_CM_004A and TP_CM_011 to fail. This problem is described in the detailed analysis, and it re-occurred several times in the UAS-PP flight test campaign. Section 6.2 Recommendations and Lessons Learned capture how this software issue was later corrected.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	11:52/3 CS Status Secure No/No-2, then UA. 11:53 - UA Send N=1, verified on CS UDMD that it was not received. 11:55 - CS Status 1/2 both links up. nominal, then UA, both links up, nominal. 11:55 - UA Status Secure No/No-2 11:56 - UA Secure Start. Confirmed (good). 11:56 - CS Status Secure: Yes/Yes-2, then on UA, both good. 11:57 - CS Status Secure Yes/Yes-2 11:57 - UA Send n=1 received ID=4. 11:58 - CS Start sending continuous data stream... then from the UA.
TP_CM_004A	User Data exchanges < MTU	**FAIL**	12:05 - UA Send n=1, then CS. Both failed 12:06 RE-trying UA Send n=1, then CS. Both failed again.
TP_CM_004A	User Data exchanges < MTU	**PASS**	12:06 Restarted DTSRs, Multiple times... 12:07 UA Secure Start. (good) on LTE. 12:07 UA Send n=1 recd id=10
TP_CM_004B	User Data exchanges > MTU	**PASS**	12:09 Taking Picture Tower_Day4Flight1_LTE (good). 12:09 Noted Auto-switchover to Satcom. 12:09 Downloading picture *LTE over Satcom. (good).
TP_CM_009	Link switchover < TET	**PASS**	12:10 CS Status 1/2 both links up, nominal. then UA, both links Up. nominal 12:11 UA. Switchover from Satcom to LTE (good). 12:11 UA Status Secure Yes/Yes-2, then on CS (both good). 12:11/12 Noted that satcom went down then came back up.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	12:12 UA Send n=1, recd id=12.
TP_CM_004B	User Data exchanges > MTU	**PASS**	12:12 Taking Picture LTE-2 (good). 12:13 Downloading picture over LTE. (good)
TP_CM_009	Link switchover < TET	**PASS**	12:13 CS Status 1/2 both links up, nominal. Then on UA, both nominal 12:13/4 UA Switchover from LTE to Satcom (good). 12:14 UA Status Secure Yes/Yes-1, then CS, Yes/Yes-1 (good)
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**FAIL**	12:15 Send n=1, both sides, UA First, both failed. 12:15 LANDED, / ON GROUND / STOPPED Spinning.

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	FAIL	12:15 CS Status Secure Yes/Yes-2 12:15 UA Status Secure Yes/Yes-1 (GUI Shows Satcom Link) 12:18 UA Send n=1, then CS both failed. 12:18 UA Secure STOP. 12:18 CS Status Secure No/No-1, then UA, No/No-1 (good). 12:18/9 UA send n=1, was not received.

Detailed Results:

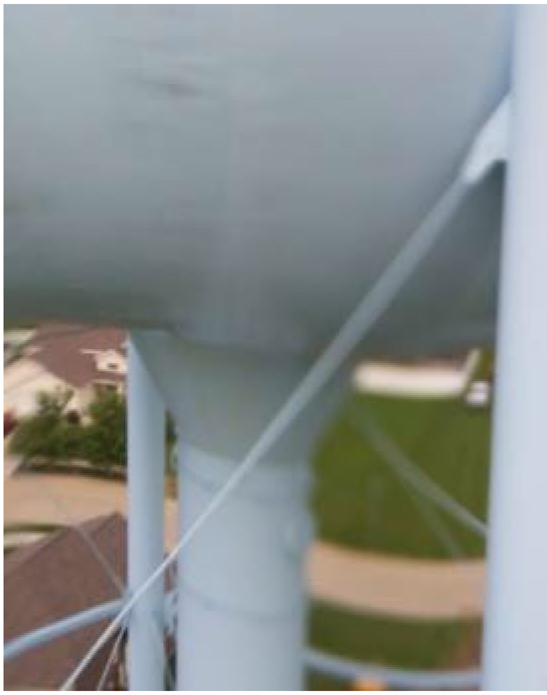


Figure 5-1. Flight 1, picture on SATCOM

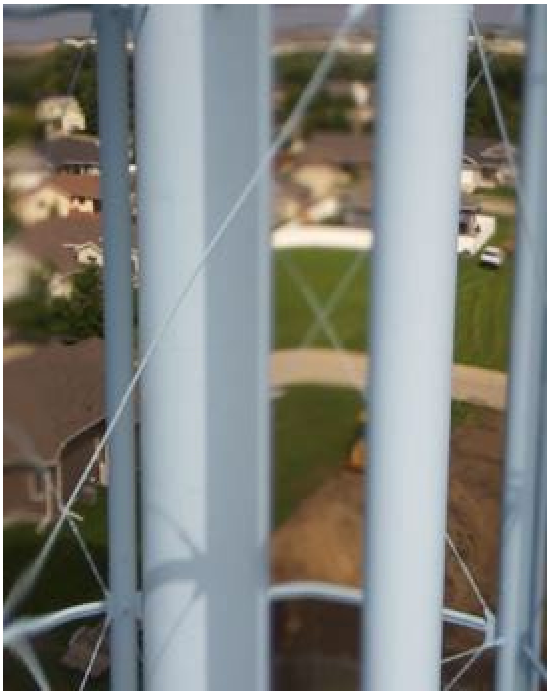


Figure 5-2. Flight 1, picture on LTE

Table 5-1. Commanded Link Switchover Times for Water Tower Flight 1

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	1	UA	24-Aug	12:11	satcom	LTE	1038	5000	Y
Water Tower	1	CS	24-Aug	12:11	satcom	LTE	408	5000	Y
Water Tower	1	UA	24-Aug	12:13	LTE	satcom	1223	5000	Y
Water Tower	1	CS	24-Aug	12:14	LTE	satcom	1701	5000	Y

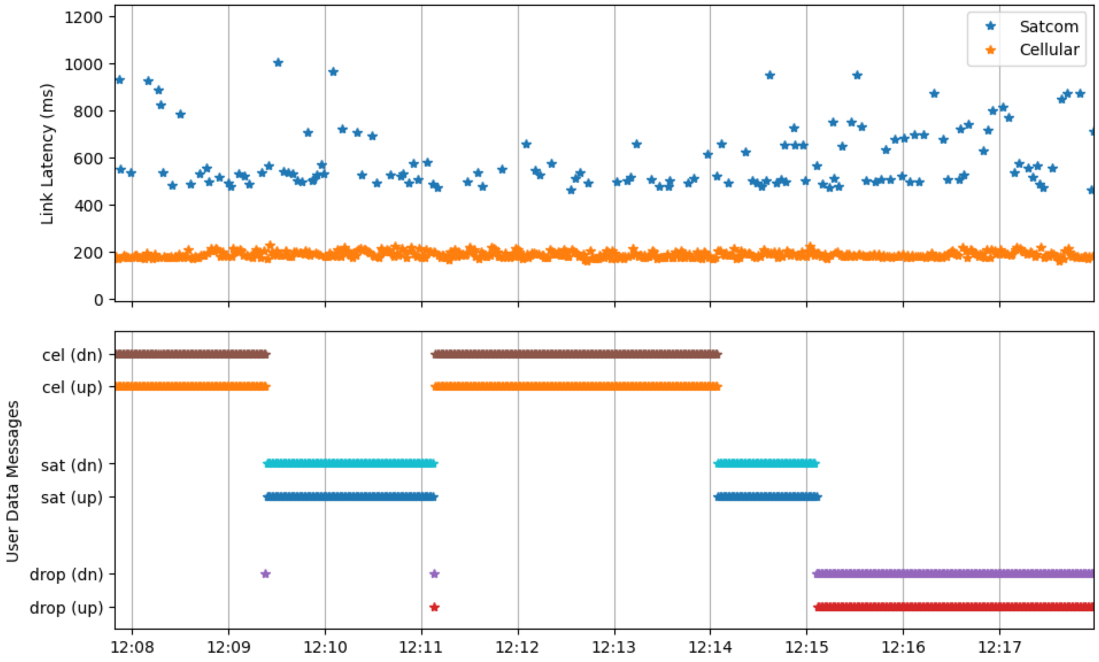


Figure 5-3. Link Latency and User Data Message Stream Path, Water Tower Flight 1

The first instance of TP_CM_004A failed because the DTSRs got out of sync.

Note 1: While the UA DTSR detects link 2 down at 17:06:46, the CS DTSR does not. This causes a tunnel switchover on the UA, while the CS is still tunneling on link 1. The CS and UA cannot talk to each other after that.

The first instance of TP_CM_004A failed because the DTSRs got out of sync.

Note 1: While the UA DTSR detects link 2 down at 17:06:46, the CS DTSR does not. This causes a tunnel switchover on the UA, while the CS is still tunneling on link 1. The CS and UA cannot talk to each other after that.

UA DTSR Log:

```
2023-08-24 16:53:25.822974 GMT INFO     UdmdIn.cpp:51               Received: ID: 00000002
Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:

2023-08-24 16:53:25.822974 GMT                                      UD-AAAAAAAAAAAAAAAAAAAA-
000002

2023-08-24 16:53:25.823477 GMT DEBUG    UserOut.cpp:76              Sending user data message to
peer

2023-08-24 16:53:25.823512 GMT WARNING  UserOut.cpp:121             Secure session disabled -
ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to

2023-08-24 16:53:25.823512 GMT                                      peer



2023-08-24 16:56:17.050080 GMT INFO     LmsfIn.cpp:159              Sending connect trigger to
remote peer

2023-08-24 16:56:17.050423 GMT INFO     LmsfIn.cpp:164              Forwarded
"CONNECT_TRIGGER.REQ     3    " to peer

2023-08-24 16:56:29.277825 GMT INFO     SessionManager.cpp:462      CONNECT completed in 11227
ms

2023-08-24 16:57:31.818437 GMT INFO     UdmdIn.cpp:51               Received: ID: 00000004
Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:

2023-08-24 16:57:31.818437 GMT                                      UD-AAAAAAAAAAAAAAAAAAAA-
000004

2023-08-24 16:57:31.818890 GMT DEBUG    UserOut.cpp:76              Sending user data message to
peer2023-08-24 16:57:31.819424 GMT DEBUG    UserOut.cpp:135             Sent "USER_DATA.REQ
66

2023-08-24 16:57:31.819424 GMT                                      ____________________________

2023-08-24 16:57:31.819424 GMT                                      040000007f000000
3f00000000000000  00fa107455000000  55442d4141414141  4141414141414141

2023-08-24 16:57:31.819424 GMT                                      414141414141412d
30303030303400]" across secure connection


2023-08-24 16:58:33.360438 GMT INFO     UserIn.cpp:96               Processing USER_DATA.REQ

2023-08-24 16:58:33.360471 GMT INFO     UserIn.cpp:115              Sent "ID: 00000022 Origin:
DTSR-CS Cmd: APP_SEND Size: 116 Rsp: FALSE Data: E" to udmd_queue


2023-08-24 17:00:03.533674 GMT INFO     LinkMonitor.cpp:168         DOWN LINK (2) timer started

2023-08-24 17:00:03.783892 GMT WARNING  LinkMonitor.cpp:202         LINK (2) is now UP. TET set
at 5000 ms. Restored in 250 ms

2023-08-24 17:06:46.144890 GMT INFO     LinkMonitor.cpp:168         DOWN LINK (2) timer started

2023-08-24 17:06:46.371176 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 2

2023-08-24 17:06:46.371197 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.


2023-08-24 17:06:46.388150 GMT WARNING  UserOut.cpp:121             Secure session disabled -
ID: 00000010 Origin: UDMD Cmd: APP_SEND Size: 144 Rsp: FALSE not sent

2023-08-24 17:06:46.388150 GMT                                      to peer

2023-08-24 17:06:47.742603 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 1
```

```
2023-08-24 17:06:47.742622 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.

2023-08-24 17:06:59.751152 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 1

2023-08-24 17:06:59.751178 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.
```

CS DTSR Log:

```
2023-08-24 16:56:16.611824 GMT INFO     OpenPeerIn.cpp:41           Received
"CONNECT_TRIGGER.REQ     3   " over open peer socket

2023-08-24 16:56:28.439506 GMT INFO     SessionManager.cpp:462      CONNECT completed in 11827
ms

2023-08-24 16:56:44.708467 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 2

2023-08-24 16:56:44.708468 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.

2023-08-24 16:56:45.063808 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 1

2023-08-24 16:56:45.063810 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.

2023-08-24 16:57:31.977470 GMT INFO     UserIn.cpp:115              Sent "ID: 00000004 Origin:
DTSR-UA Cmd: SEND Size: 63 Rsp: FALSE Data:

2023-08-24 16:57:31.977470 GMT                                      UD-AAAAAAAAAAAAAAAAAAAA-
000004" to udmd_queue

2023-08-24 16:58:33.060587 GMT DEBUG    UserOut.cpp:135             Sent "USER_DATA.REQ
119

2023-08-24 16:58:33.060587 GMT

2023-08-24 16:58:33.060587 GMT                                      d

2023-08-24 16:58:33.060587 GMT                                      d

2023-08-24 16:58:33.060587 GMT                                      0d00000000000000
7400000000000000  0000000000000000  4500005421e84000  401103e70a640002

2023-08-24 16:58:33.060587 GMT                                      0a640001ad4ed897
0040ac9101000000  30000000fd040000  7ead001400000602  01011df6fd040000

2023-08-24 16:58:33.060587 GMT                                      7fad001400000902
010170c9fd040000  80ad001400000b02  0101650f]" across secure connection

2023-08-24 17:00:03.578086 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 2

2023-08-24 17:00:03.578087 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.
```

No link down detected @ 17:06:46.

The final instance of TP_CM_004A and TP_CM_011 fail because the DTSRs get out of sync again.

Note 2: The UA DTSR detected link 1 down at 17:05:07, while the CS DTSR did not. The CS DTSR will continue to tunnel through link 1, while the UA does it through link 2. The CS and UA cannot talk to each other after that.

UA DTSR Log:

```
2023-08-24 17:15:07.075222 GMT INFO     LinkManager.cpp:208         Detected link DOWN: 1

2023-08-24 17:15:07.075223 GMT INFO     LinkManager.cpp:212         Lost link for secure
connection. Initiating switchover.
```

CS DTSR Log:

No link down detected at 17:15:07.

5.1.2 Target A – Water Tower – Flight 2-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	2	24 Aug 2023	1:01 CDT	1:15 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	1:01 CS Status Secure No/No-2, then UA, same both. 1:02 UA send n=1, not received - good 1:02 CS Status 1/2, both links up. good., then UA, both links up. nominal. 1:02 UA Secure Start. good on LTE. 1:03 CS Status Secure Yes/Yes-2. then UA. 1:03/4 CS started sending user data stream, then UA.
TP_CM_004A	User Data exchanges < MTU	PASS	1:05 ARMING / SPINNING / TAKEOFF 1:05 UA Send n=1, recd id=4, then CS, recd id=2
TP_CM_004B	User Data exchanges > MTU	PASS	1:06 Taking picture Day4Flight2-LTE. then downloaded. good.
TP_CM_004A	User Data exchanges < MTU	PASS	1:07 uA Send n=1, recd id=6.
TP_CM_009	Link switchover < TET	PASS	1:07 CS Status 1/2 both links up, then UA: both links up nominal - good. 1:07 UA Switch from LTE to Satcom . good. 1:08 UA Status Secure Yes/Yes-1, then CS. Yes/Yes-1 - good - both on Satcom.
TP_CM_007	Control message exchanges	PASS	
TP_CM_004B	User Data exchanges > MTU	PASS	1:09 Taking picture 2 Day4Flight2-Satcom. Downloading. good. 1:10 finished download.
TP_CM_004A	User Data exchanges < MTU	PASS	1:10 UA send n=1, recd id=8.
TP_CM_009	Link switchover < TET	PASS	1:10 CS Status 1/2 both links up, nominal. the UA, both links up. nominal. - good 1:10 UA Switch 2. switchover from Satcom to LTE. - good. 1:11 UA status Secure Yes/Yes-2, then CS, Yes/Yes-2 (LTE) - good.
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	1:11 Hon issued cleared to land. 1:12 send n=1 recd id=10, then CS, recd id=4.
TP_CM_004A	User Data exchanges < MTU	PASS	1:12 LANDED / ON GROUND / STOPPED SPINNING. end of flight #2 1:12 UA Send n=1, recd id=12, 1:14 CS send n=1, recd id=6.

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	PASS	1:14 UA status Secure, Yes/Yes-2 (satcom). 1:15 CS status Secure, Yes/Yes-2 (satcom). 1:15 UA Secure Stop. 1:15 CS status Secure No/No-2, then UA, No/No-2. 1:15 UA send n=1 confirmed nothing recd.

Detailed Results:

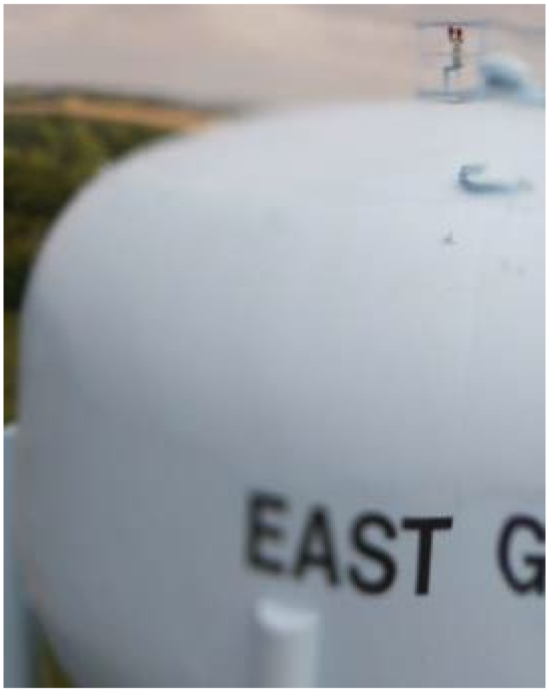


Figure 5-4. Flight 2, picture on LTE

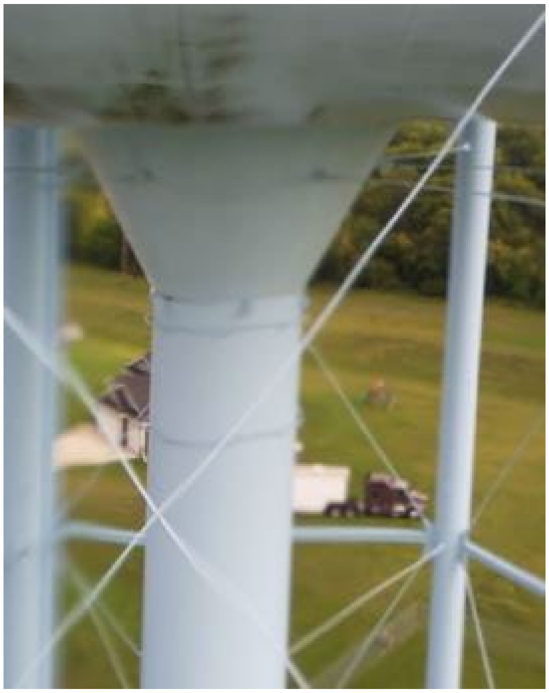


Figure 5-5. Flight 2, picture on SATCOM

Table 5-2. Commanded Link Switchover Times for Water Tower Flight 2

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	2	UA	24-Aug	1:07	LTE	satcom	1258	5000	Y
Water Tower	2	CS	24-Aug	1:07	LTE	satcom	1817	5000	Y
Water Tower	2	UA	24-Aug	1:10	satcom	LTE	797	5000	Y
Water Tower	2	CS	24-Aug	1:10	satcom	LTE	362	5000	Y

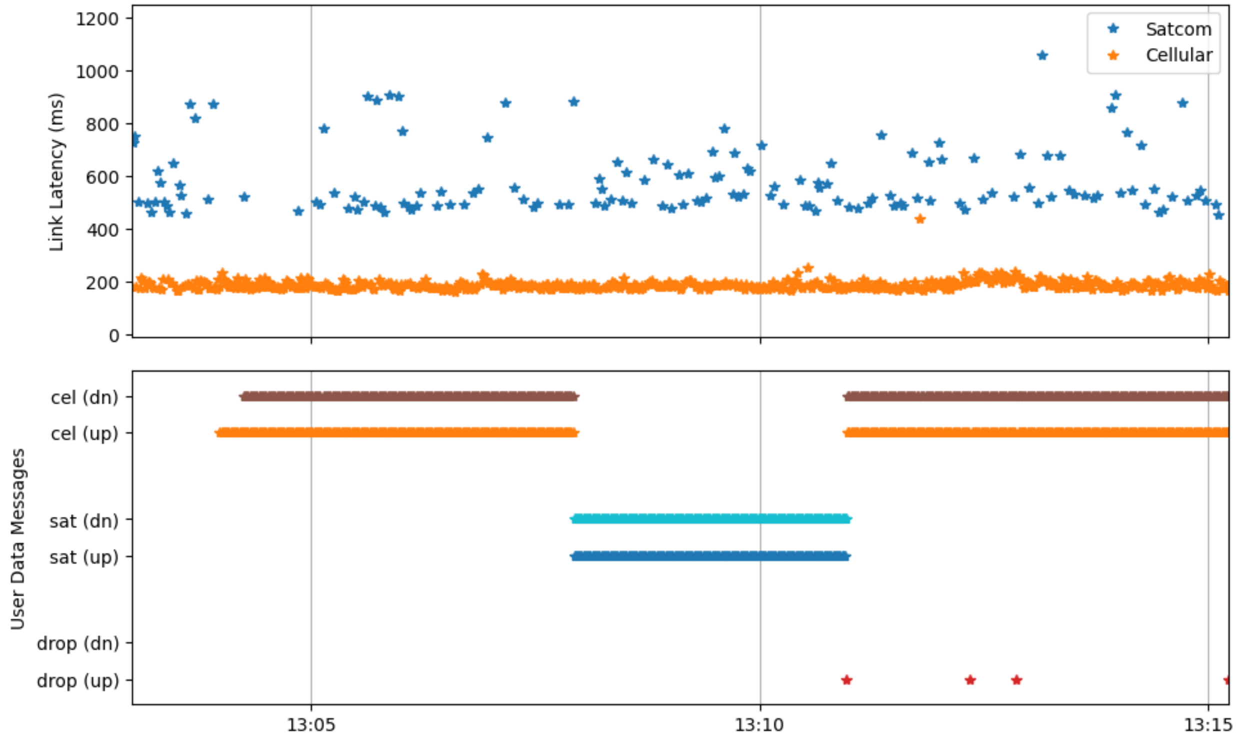


Figure 5-6. Link Latency and User Data Message Stream Path, Water Tower Flight 2

5.1.3 Target A – Water Tower – Flight 3-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	3	24 Aug 2023	1:25 CDT	1:38 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	1:25 CS Status Secure No/No-2, then UA, same No/No-2. -good. 1:25 UA Send n=1, not recd. - good. 1:25 CS Status 1/2, both links up, nominal. 1:26 UA Status 1/2, both links up, nominal. 1:25 UA Secure Start.. - good session established on LTE. 1:26 CS Status Secure Yes/Yes-2 - good, then UA, Yes/Yes-2 - good. 1:27 CS Starting continuous user data stream. then UA.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:29 ARMING / SPINNING / TAKEOFF Flight #3 1:29 UA send n=1 UA recd id=4, then CS, recd id=2.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:30 Taking Picture, day4flight3-LTE. - good over LTE. then Downloading... -good.
TP_CM_009	Link switchover < TET	**PASS**	1:31 CS Status 1/2 both links up, nominal - good, then UA, both links up, nominal. 1:31 UA Switchover from LTE to Satcom - good. 1:32 UA Status Secure Yes/Yes-1, then CS, Yes/Yes-1. - good on Satcom.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:32 UA Send n=1, recd id=6.
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:33 Taking Picture day4flight3-Satcom. - good.
TP_CM_009	Link switchover < TET	**PASS**	1:34 CS Status 1/2 both links up, nominal. then UA: both links up, nominal. - good. 1:34 Switchover from Satcom to LTE - good. 1:34/5 UA Status Secure Yes/Yes-2 1:35 CS Status Secure Yes/Yes-2
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:35 UA send n=1, recd id=8
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:36 UA send n=1 recd id=10, then CS, recd id = 4 - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:36 LANDED / ON GROUND / STOPPED. END OF FLIGHT #3 1:36/7 UA Send n=1 recd id=12, then CS, recd id=6 - good.
TP_CM_011	Control / User Plane Termination	**PASS**	1:37 CS Status Secure Yes/Yes-2, then UA, Yes/Yes-2 - good. 1:37 UA Secure Stop. 1:38 CS Status Secure No/No-2, then UA, No/No-2 - good 1:38 UA send n=1, not recd - good.

Detailed Results:

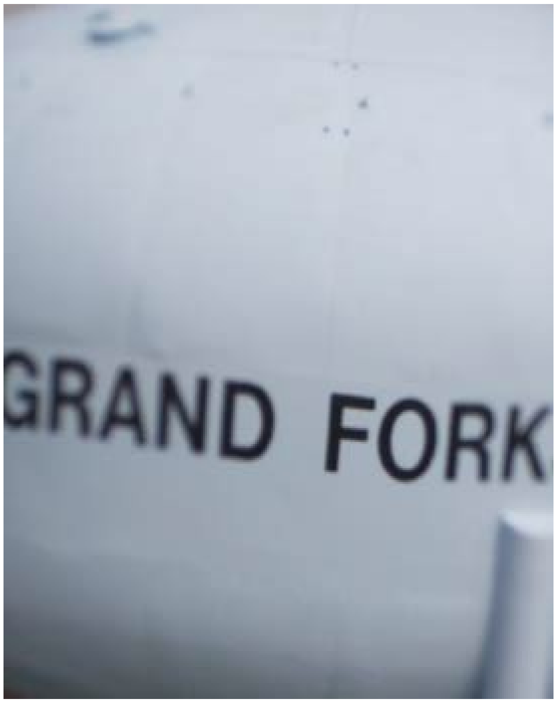


Figure 5-7. Flight 3, picture on LTE

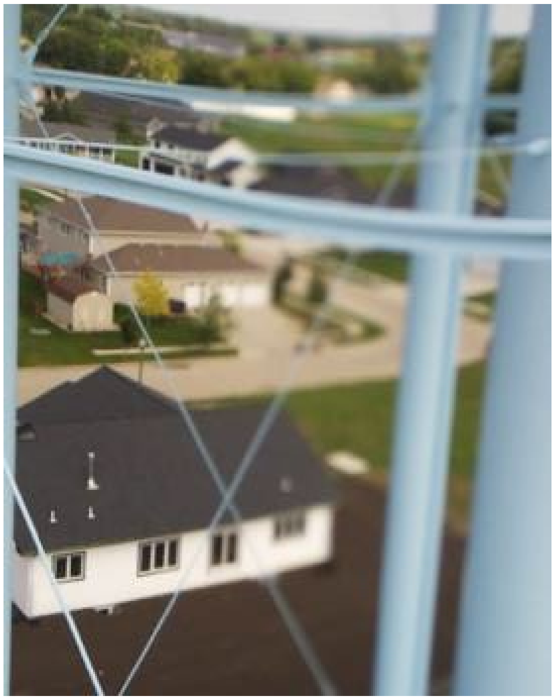


Figure 5-8. Flight 3, picture on satcom

Table 5-3. Commanded Link Switchover Times for Water Tower Flight 3

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	3	UA	24-Aug	1:31	LTE	satcom	1135	5000	Y
Water Tower	3	CS	24-Aug	1:31	LTE	satcom	1331	5000	Y
Water Tower	3	UA	24-Aug	1:34	satcom	LTE	824	5000	Y
Water Tower	3	CS	24-Aug	1:34	satcom	LTE	367	5000	Y

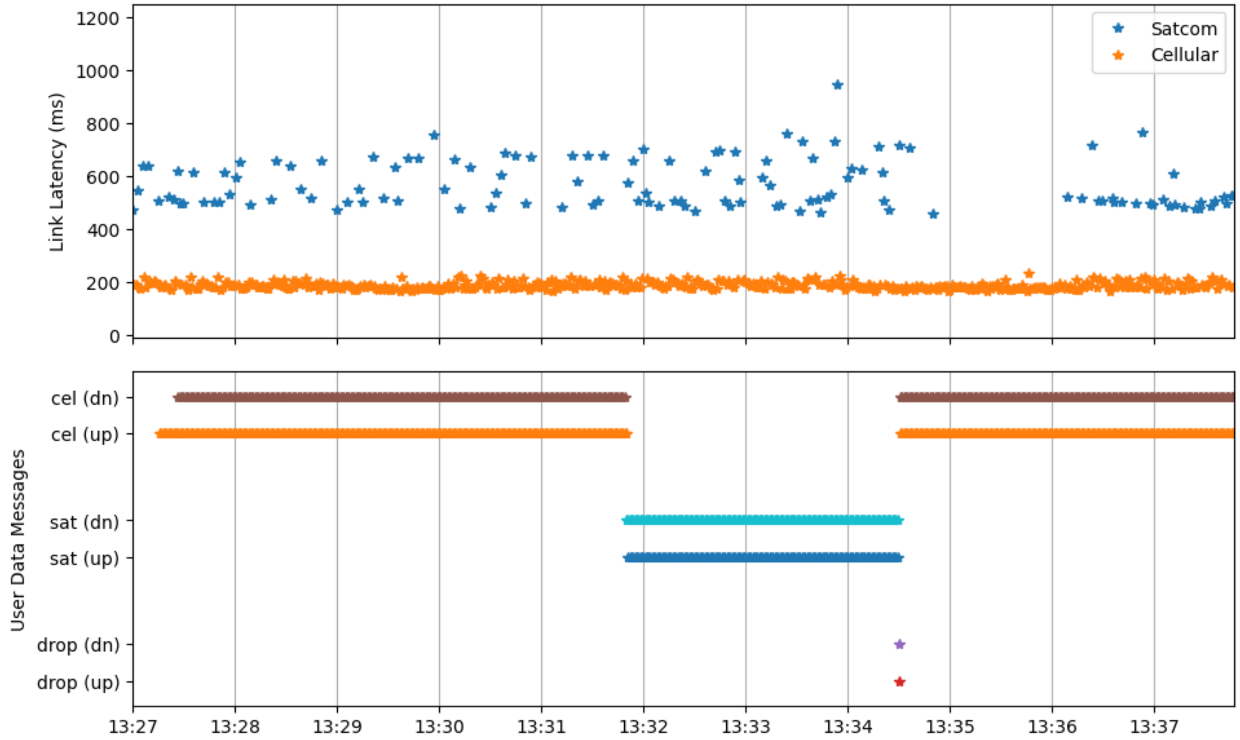


Figure 5-9. Link Latency and User Data Message Stream Path, Water Tower Flight 3

5.1.4 Target A – Water Tower – Flight 4-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	4	24 Aug 2023	1:51 CDT	1:38 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	1:51 CS Status Secure No/No-2, then UA, No/No-2 - good. 1:51 UA send n=1 not recd - good. 1:51 CS Status 1/2 both links up nominal 1:52 UA Status 1/2 both links up nominal 1:52 UA Secure Start - good on LTE seen on GUI. 1:52 CS Status Secure Yes/Yes-2, then UA, Yes/Yes-2. - good. 1:53 CS Start sending user data stream - good. then UA. - good.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:55-ish ARMING / TAKEOFF / SPINNING 1:56 UA Send n=1 recd id=6, then CS, ID = 2
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:57 Taking picture Day 4 Flight 4 LTE, - good then downloading - good.
TP_CM_009	Link switchover < TET	**PASS**	1:57 CS Status 1/2 both links up, nominal, then UA, - good. 1:58 Switchover from LTE to Satcom - good. 1:58 UA Status Secure Yes/Yes-1, then CS Yes/Yes-1 - good. NOTED that LTE Went down then UP, no impact.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:58/9 Send n=1, recd - good.
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:59 Taking picture over satcom - day4 flight4 satcom - good. Downloading... - good.
TP_CM_009	Link switchover < TET	**PASS**	2:00 CS Status 1/2 both links up nominal - good. then UA both links up nominal - good. 2:00 Switchover from Satcom to LTE - good. 2:00 UA Status Secure Yes/Yes-2 LTE., then CS, Yes/Yes-2 LTE - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:01 cleared for landing 2:01 Send n=1 recd id=10, then CS recd id=4
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:02 LANDED / ON GROUND / 2:02 Send n=1 recd id=12, then CS recd id=6
TP_CM_011	Control / User Plane Termination	**PASS**	2:02 CS Status Secure Yes/Yes-2 LTE - good, then UA same Yes/Yes-2 - good. 2:03 Secure Stop - good 2:03 CS Status Secure No/No-2, then UA, No/No-2, - good 2:03 UA send n=1, not recd - good.

Detailed Results:

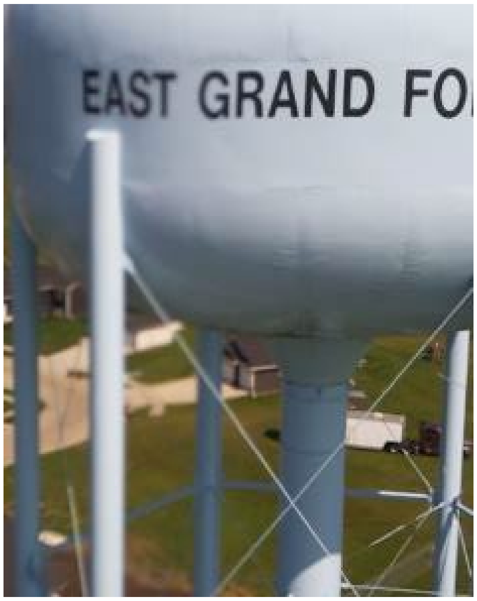


Figure 5-10. Flight 4, picture on LTE

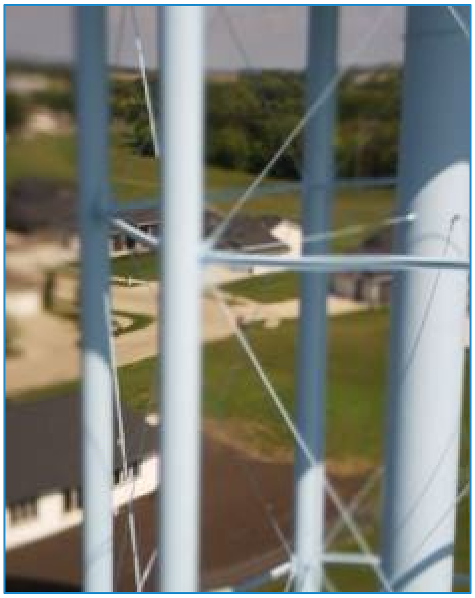


Figure 5-11. Flight 4, picture on SATCOM

Table 5-4. Commanded Link Switchover Times for Water Tower Flight 4

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	4	UA	24-Aug	1:58	LTE	satcom	1146	5000	Y
Water Tower	4	CS	24-Aug	1:58	LTE	satcom	1853	5000	Y
Water Tower	4	UA	24-Aug	2:00	satcom	LTE	851	5000	Y
Water Tower	4	CS	24-Aug	2:00	satcom	LTE	412	5000	Y

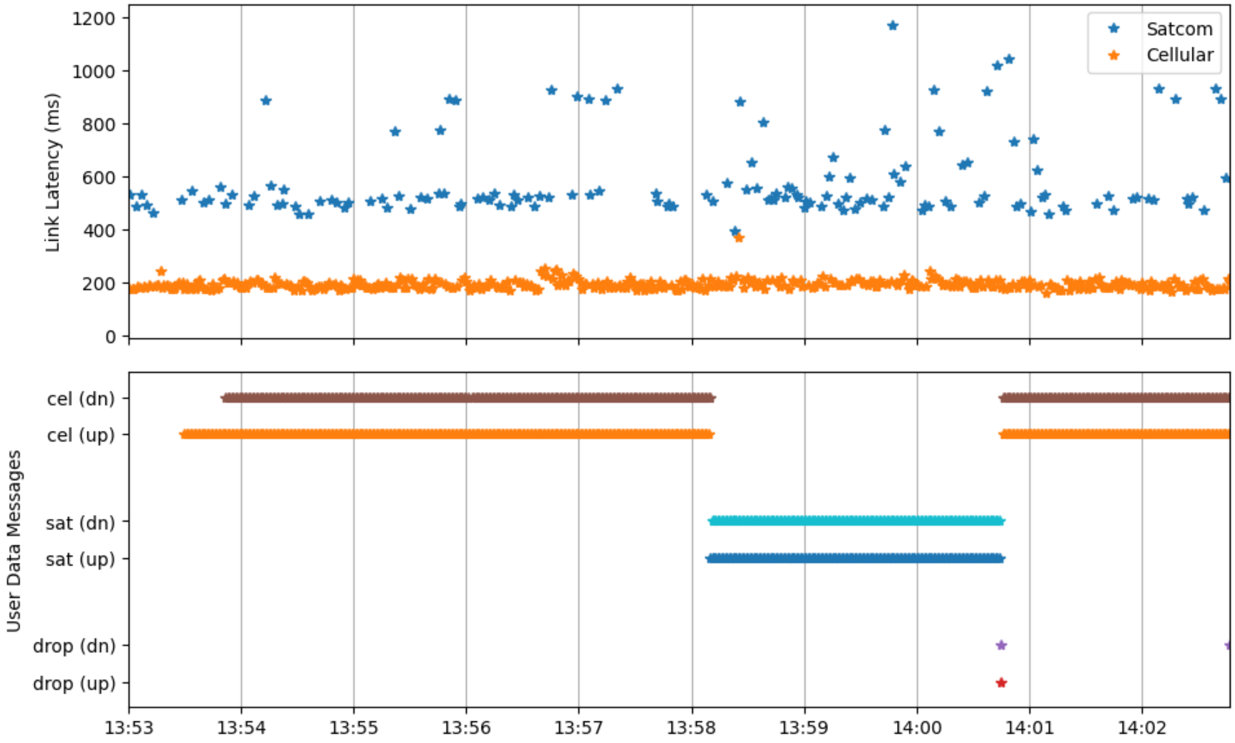


Figure 5-12. Link Latency and User Data Message Stream Path, Water Tower Flight 4

5.1.5 Target A – Water Tower – Flight 5-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

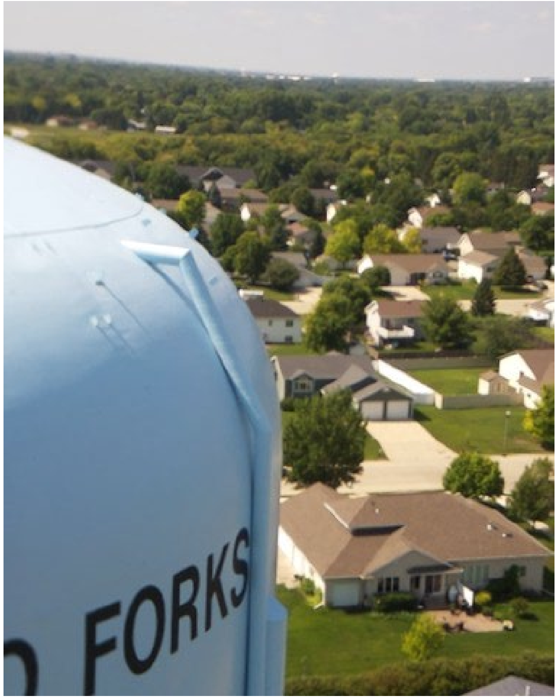
Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	5	24 Aug 2023	2:14 CDT	2:29 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	2:14 CS Status Secure No/No-2, then UA, same - good. 2:15 UA send n=1, not recd - good. 2:15 CS Status 1/2 both links up, nominal. then UA same - good. 2:15 UA Secure Start - good connected on LTE. 2:15 CS Status Secure Yes/Yes-2 LTE. 2:16 UA Status Secure Yes/Yes-2 LTE. 2:16 CS Starting continuous user data stream - good. then UA. - good.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:18 ARMING / SPINNING / TAKEOFF 2:18 UA Send n=1 recd id=4, then CS, recd ID=2 - good
TP_CM_004B	User Data exchanges > MTU	**PASS**	2:19 Taking Picture on LTE Day4 Flight 5 LTE 2:20 Downloading Picture on LTE Day4 Flight 5 LTE
TP_CM_009	Link switchover < TET	**PASS**	2:20 CS Status 1/2 both links up, nominal good, then UA both links up, nominal - good 2:20 Switchover from LTE to Satcom - good. 2:20 UA Status Secure Yes/Yes-1 - good. 2:21 CS Status Secure Yes/Yes-1 - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:21 UA send n=1, recd id=6,
TP_CM_004B	User Data exchanges > MTU	**PASS**	2:22 Taking Picture Day4 Flight5 - Satcom 2:22/23 NOTED Automatic Switchover to LTE!! GUI shows LTE 2:23 Switchover from LTE to Satcom - good. GUI shows Satcom now. 2:23 Downloading Picture over Satcom... 2:24 Download complete. over satcom.
TP_CM_009	Link switchover < TET	**PASS**	2:24 CS Status 1/2 both links up, nominal - good, then UA same, good. 2:24 Switchover from Satcom to LTE. 2:25 UA status Secure Yes/Yes-2, then CS Yes/Yes-2 LTE - good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:26 UA send n=1 recd id=8, then CS recd id=4. 2:26 LANDED / ON GROUND /
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:26 Noted auto switchover. Now on Satcom. GUI shows satcom 2:26/27 UA Send n=1 recd id=10.
TP_CM_011	Control / User Plane Termination	**PASS**	2:28 CS Status Secure Yes/Yes-1. then UA Yes/Yes-1 - good. 2:28 UA Secure Stop. Noted LTE is dropping and coming back. 2:28/9 CS Status Secure No/No-1. 2:29 UA Status Secure No/No-1. 2:29 UA send n=1, not recd - good.

Detailed Results:



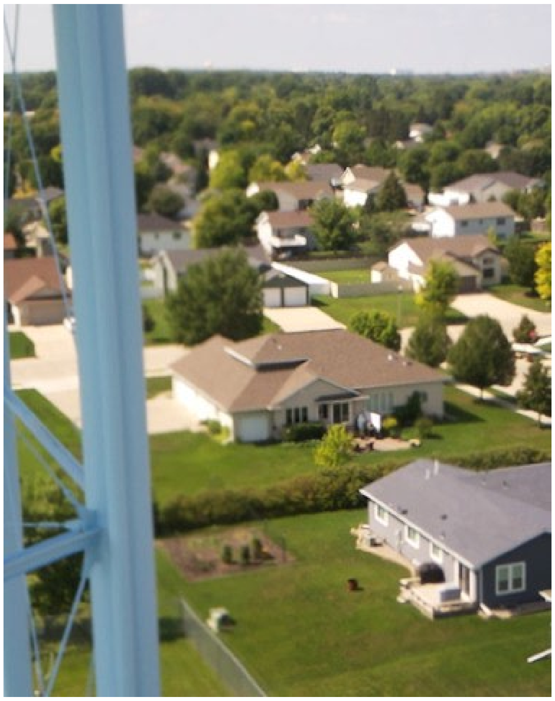


Figure 5-13. Flight 5, picture sent on LTE

Figure 5-14. Flight 5, picture sent on SATCOM

Table 5-5. Commanded Link Switchover Times for Water Tower Flight 5

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	5	UA	24-Aug	2:20	LTE	satcom	1995	5000	Y
Water Tower	5	CS	24-Aug	2:20	LTE	satcom	1606	5000	Y
Water Tower	5	UA	24-Aug	2:24	satcom	LTE	1844	5000	Y
Water Tower	5	CS	24-Aug	2:24	satcom	LTE	391	5000	Y

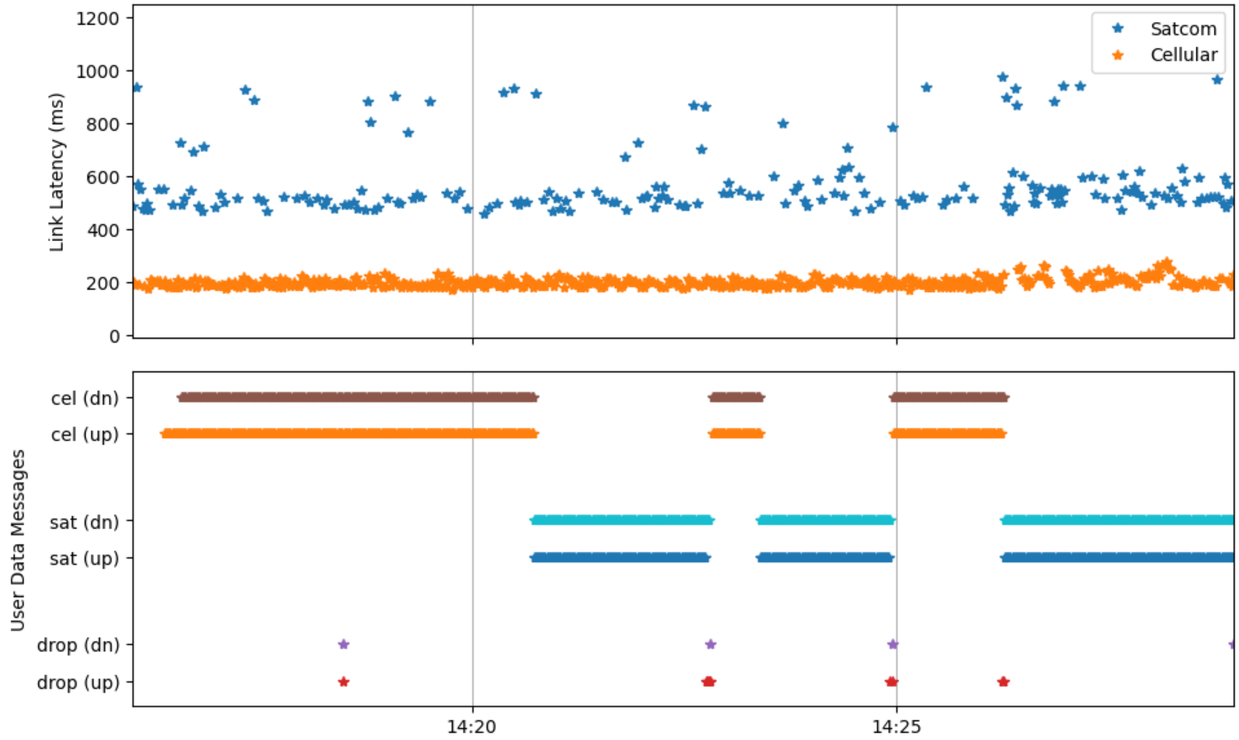


Figure 5-15. Link Latency and User Data Message Stream Path, Water Tower Flight 5

5.1.6 Target A – Water Tower – Flight 6-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
A-1	FTS-1 – Target A (Water Tower), Nominal tests, with encryption	6	24 Aug 2023	2:48 CDT	3:01 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	2:48 CS Status Secure No/No-2, then UA No/No-2 - good. 2:48 UA Send n=1, nothing recd. - good. 2:48 CS Status 1/2 both links up. nominal. then UA, both up nominal -good. 2:49 UA Secure Start - good session on LTE. 2:49 CS Status Secure Yes/Yes-2, then UA, Yes/Yes-2 LTE - good. 2:49 CS Started sending continuous user data stream 2:50 UA Started sending continuous user data stream

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:52 ARMING / SPINNING / TAKEOFF Flight #6 2:52 UA Send n=1 recd ID=4, then CS recd id=2 - good.
TP_CM_004B	User Data exchanges > MTU	**PASS**	2:53 Taking Picture Day4 flight 6 LTE. ERROR / FOCUSING CAMERA. Re-positioned to farther away and looking at letters. 2:55 Taking Picture Try-3, - good. 2:55/56 downloaded. - good.
TP_CM_009	Link switchover < TET	**PASS**	2:56 CS Status 1/2 then UA both good nominal - good. 2:56 Switch from LTE to Satcom - good. 2:56 Status Secure Yes/Yes-1, then UA - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:57- UA Send n-1 recd id=6
TP_CM_004B	User Data exchanges > MTU	**PASS**	2:57 Taking picture Day4 flight6 satcom - good. 2:58 Downloading picture - Satcom - good.
TP_CM_009	Link switchover < TET	**PASS**	2:58 CS Status 1/2 both links up, nominal. then UA both links up, nominal 2:59 2:59 UA Switchover from Satcom to LTE - good. 2:59 UA Status Secure Yes/Yes-2 LTE, then CS Status Secure Yes/Yes-2. LTE - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	2:59 cleared to land. 2:59 UA Send n=1 recd id=8, then CS recd id=4.
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:00 LANDED / ON GROUND / STOPPED 3:00 UA Send n=1 recd id=10, then CS, id=6.
TP_CM_011	Control / User Plane Termination	**PASS**	3:01 CS Status Secure Yes/Yes-2 LTE. then UA, Yes/Yes-2 LTE good. 3:01 UA Secure Stop. - good. 3:01 CS Status Secure No/No-2, then UA, No/No-2 - good. 3:01 UA Send n=1, not recd. - good.

Detailed Results:

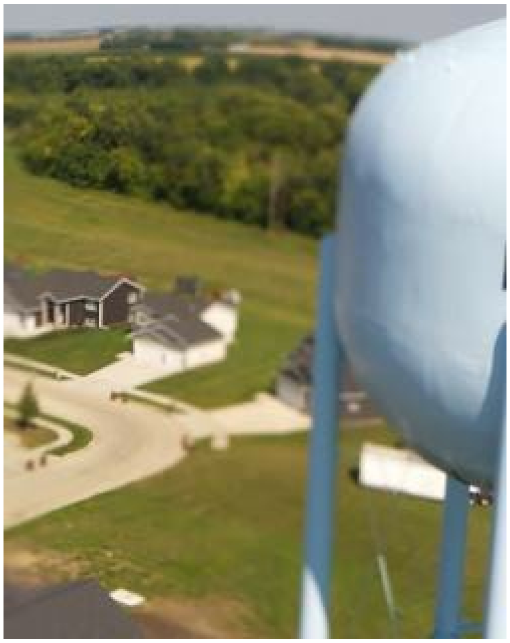


Figure 5-16. Flight 6, picture on LTE

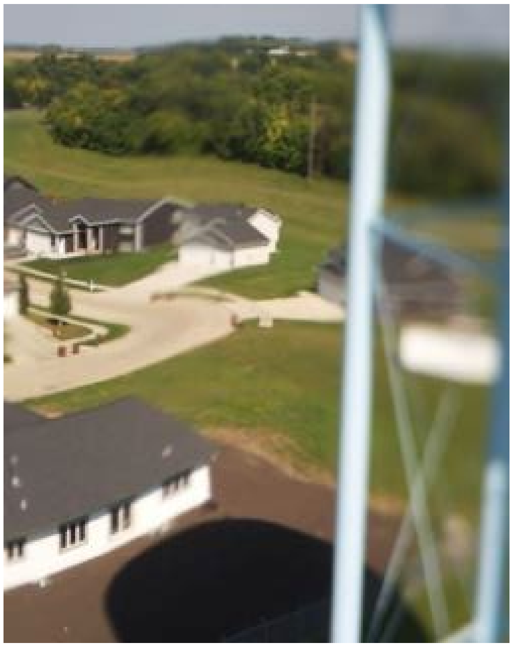


Figure 5-17. Flight 6, picture on SATCOM

Table 5-6. Commanded Link Switchover Times for Water Tower Flight 6

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	5	UA	24-Aug	2:20	LTE	satcom	1995	5000	Y
Water Tower	5	CS	24-Aug	2:20	LTE	satcom	1606	5000	Y
Water Tower	5	UA	24-Aug	2:24	satcom	LTE	1844	5000	Y
Water Tower	5	CS	24-Aug	2:24	satcom	LTE	391	5000	Y

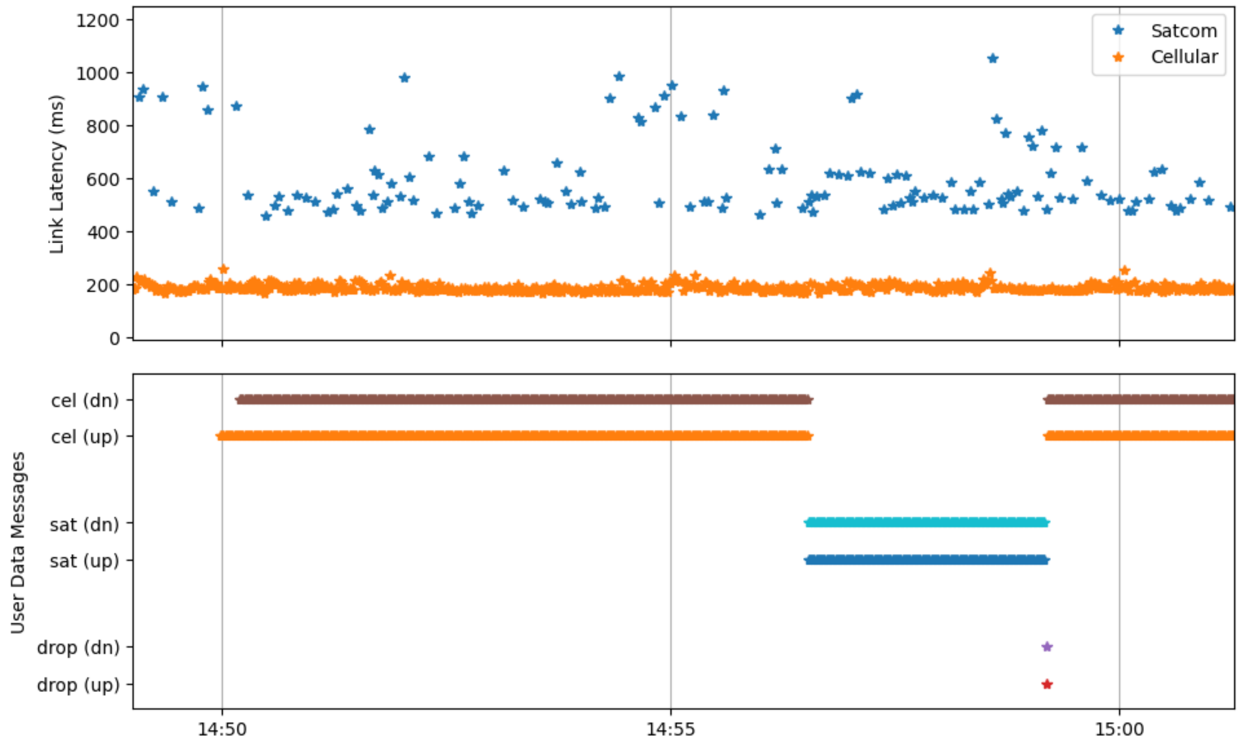


Figure 5-18. Link Latency and User Data Message Stream Path, Water Tower Flight 6

5.1.7 Target B – Walking Path – Flight 1-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	1	24 Aug 2023	3:46 CDT	3:58 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	3:46 CS Status Secure No/No-2 then UA same - good. 3:46 UA send n=1, not recd - good. 3:46 CS Status 1/2, both links up, nominal, - good, then UA same -good. 3:47 UA Secure Start - good. GUI Shows LTE secure. 3:47 CS Status Secure Yes/Yes-2, then UA same - good. 3:48 CS Started sending continuous data stream , then from UA - good.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:49 TAKEOFF Flight 1 walking path. 3:49 UA Send n=1 recd id=4, then CS recd id=2.
TP_CM_004B	User Data exchanges > MTU	**PASS**	3:50 Taking picture walking-day4-flight1 - LTE. 3:50/1 Downloading Picture - good.
TP_CM_009	Link switchover < TET	**PASS**	3:51 CS Status 1/2 both links up, nominal - good then UA - both good 3:51 Switchover from LTE to Satcom - good 3:51 UA Status Secure Yes/Yes-1, then CS - good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:52 UA Send n=1, recd id=6.
TP_CM_004B	User Data exchanges > MTU	**PASS**	3:52 Taking picture over satcom. – good 3:53 Downloading picture over satcom - good
TP_CM_009	Link switchover < TET	**PASS**	3:53 CS Status 1/2 both links up, nominal 3:54 UA Status 1/2 both links up, nominal - good 3:54 Switchover from Satcom to LTE 3:54 UA Status Secure Yes/Yes-2, then CS same good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:54 UA send n=1 recd id=8. 3:55 UA send n=1 id=10, then CS recd id=4 good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:55 Noticed Satcom link went down due to long latency over 2 seconds. 3:56 LANDED / ON GROUND / STOPPED 3:56 send n=1 recd id=12.
TP_CM_011	Control / User Plane Termination	**PASS**	3:56/7 CS Status Secure Yes/Yes-2 3:57 UA Status Secure Yes/Yes-2 good 3:57 UA Secure Stop 3:57 CS Status Secure No/No-2, then UA same - good. 3:57/7 UA send n=1 - not recd - good.

Detailed Results:

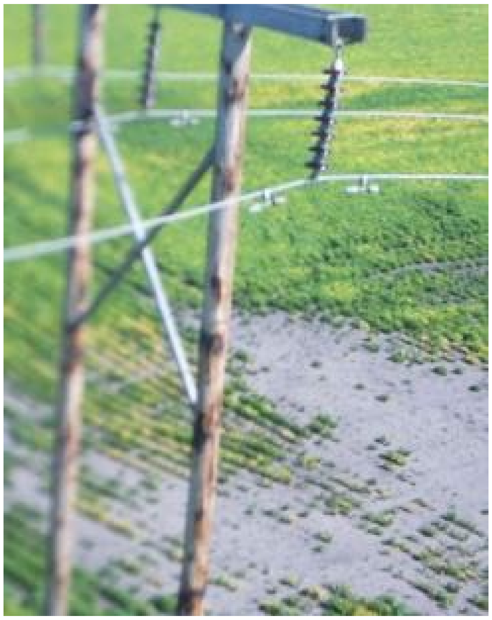


Figure 5-19. Flight 1, picture on LTE

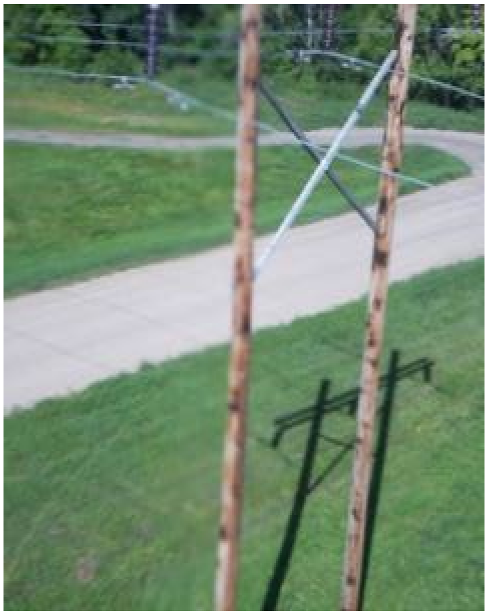


Figure 5-20. Flight 1, picture on SATCOM

Table 5-7. Commanded Link Switchover Times for Walking Path Flight 1

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	1	UA	24-Aug	3:51	LTE	satcom	1120	5000	Y
Walking Path	1	CS	24-Aug	3:51	LTE	satcom	1030	5000	Y
Walking Path	1	UA	24-Aug	3:54	satcom	LTE	858	5000	Y
Walking Path	1	CS	24-Aug	3:54	satcom	LTE	399	5000	Y

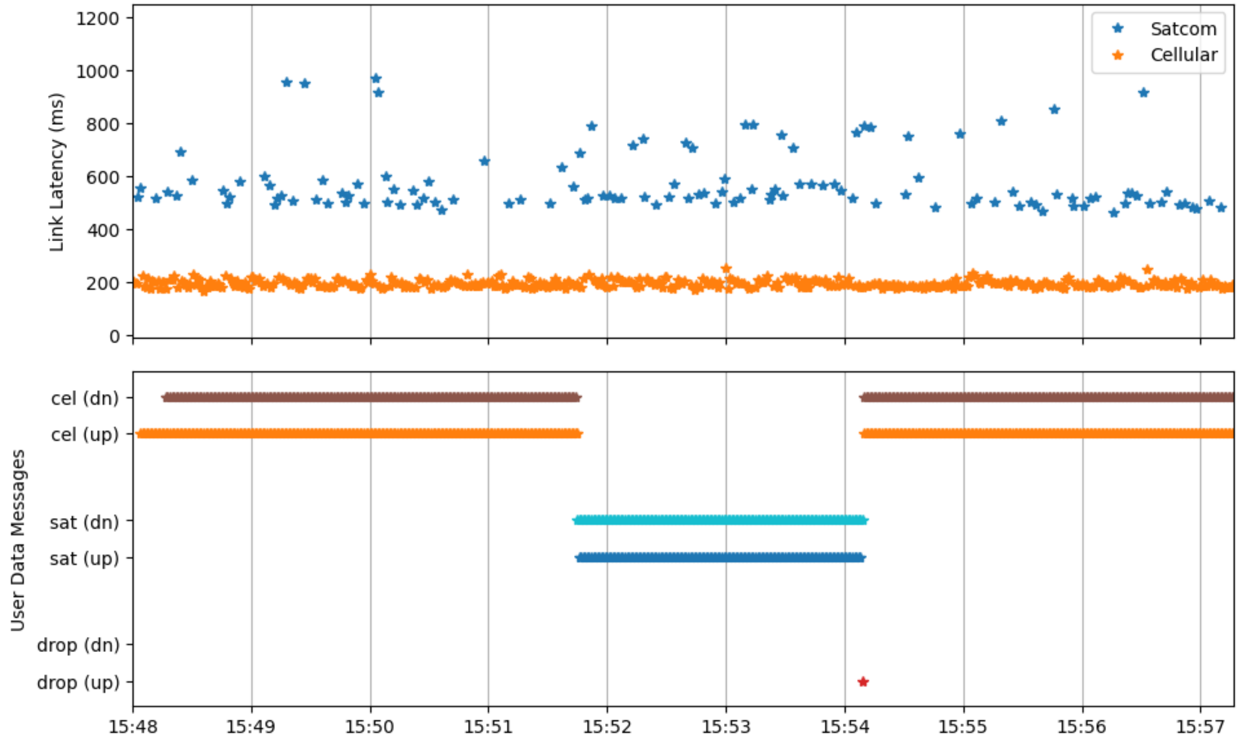


Figure 5-21. Link Latency and User Data Message Stream Path, Walking Path Flight 1

5.1.8 Target B – Walking Path – Flight 2-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	2	24 Aug 2023	4:10 CDT	4:22 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	🟩PASS	4:10 Ready to start PROCEDURE Flight #2 - walking. 4:10 CS Status Secure No/No-2, then UA, same - good. 4:10 UA send n=1 not recd - good. 4:11 CS Status 1/2 both links up, nominal. good, then UA, same - good. 4:11 UA Secure Start - Session came up on LTE. - good. 4:11 CS Status Secure Yes/Yes-2, then UA same - good. 4:12 CS starting sending continuous data stream. then UA - good.
TP_CM_004A	User Data exchanges < MTU	🟩PASS	4:12 cleared for takeoff. 4:14 UA issued n=1 recd id=4, then CS n=1 recd id=2.
TP_CM_004B	User Data exchanges > MTU	🟩PASS	4:14 noticed auto-switchover to satcom. 4:15 Switchover from Satcom to LTE. 4:15 Taking Picture - good. 4:15 Downloaded picture over LTE.
TP_CM_007	Control message exchanges	🟩PASS	
TP_CM_009	Link switchover < TET	🟩PASS	4:16 CS Status 1/2 both links up. 4:16 switchover to Satcom. 4:17 UA Status 1/2 both links up nominal.
TP_CM_007	Control message exchanges	🟩PASS	
TP_CM_004B	User Data exchanges > MTU	🟩PASS	4:18 Taking picture walking day4 flight2 satcom. good. then Downloaded over Satcom.
TP_CM_009	Link switchover < TET	🟩PASS	4:19 CS Status 1/2 both links up. nominal. good. then UA status 1/2 both links up. nominal good. 4:19 Switchover from Satcom to LTE. - good. 4:19 UA Status Secure Yes/Yes-2, then CS Yes/Yes-2 good.
TP_CM_007	Control message exchanges	🟩PASS	
TP_CM_004A	User Data exchanges < MTU	🟩PASS	4:20 UA Send n=1 recd id=6 4:20 UA Send n=1 recd id=8, then CS id=4
TP_CM_004A	User Data exchanges < MTU	🟩PASS	4:20/1 LANDED / ON GROUND / STOPPED SPINNING End of FLIGHT #2. 4:21 UA send n=1 recd id=10, then CS id=6
TP_CM_011	Control / User Plane Termination	🟩PASS	4:21 CS Status secure Yes/Yes-2 then UA same, good. 4:21 UA Secure Stop - good. 4:21 CS Status Secure No/No-2 good 4:22 UA Status Secure No/No-2 4:22 UA Send n=1 not recd - good.

Detailed Results:

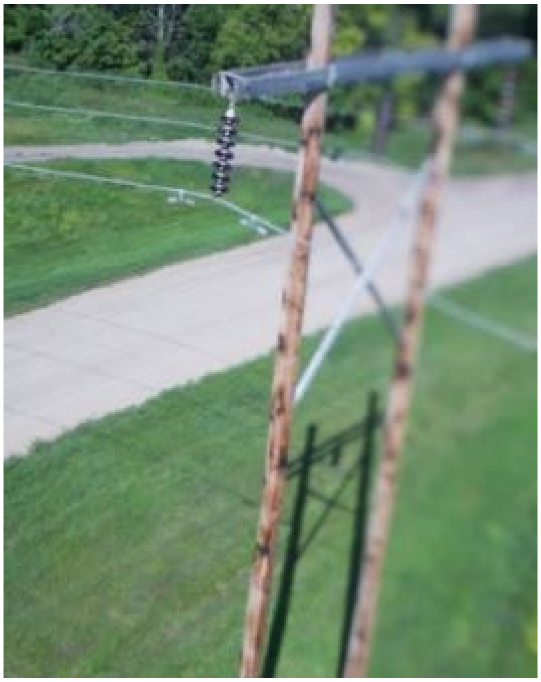


Figure 5-22. Flight 2, picture on LTE

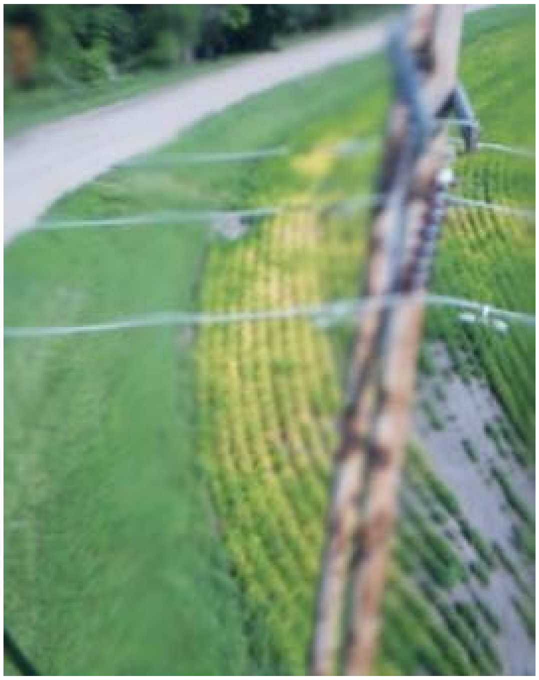


Figure 5-23. Flight 2, picture on SATCOM

Table 5-8. Commanded Link Switchover Times for Walking Path Flight 2

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	2	UA	24-Aug	4:15	satcom	LTE	798	5000	Y
Walking Path	2	CS	24-Aug	4:15	satcom	LTE	484	5000	Y
Walking Path	2	UA	24-Aug	4:19	satcom	LTE	795	5000	Y
Walking Path	2	CS	24-Aug	4:19	satcom	LTE	345	5000	Y

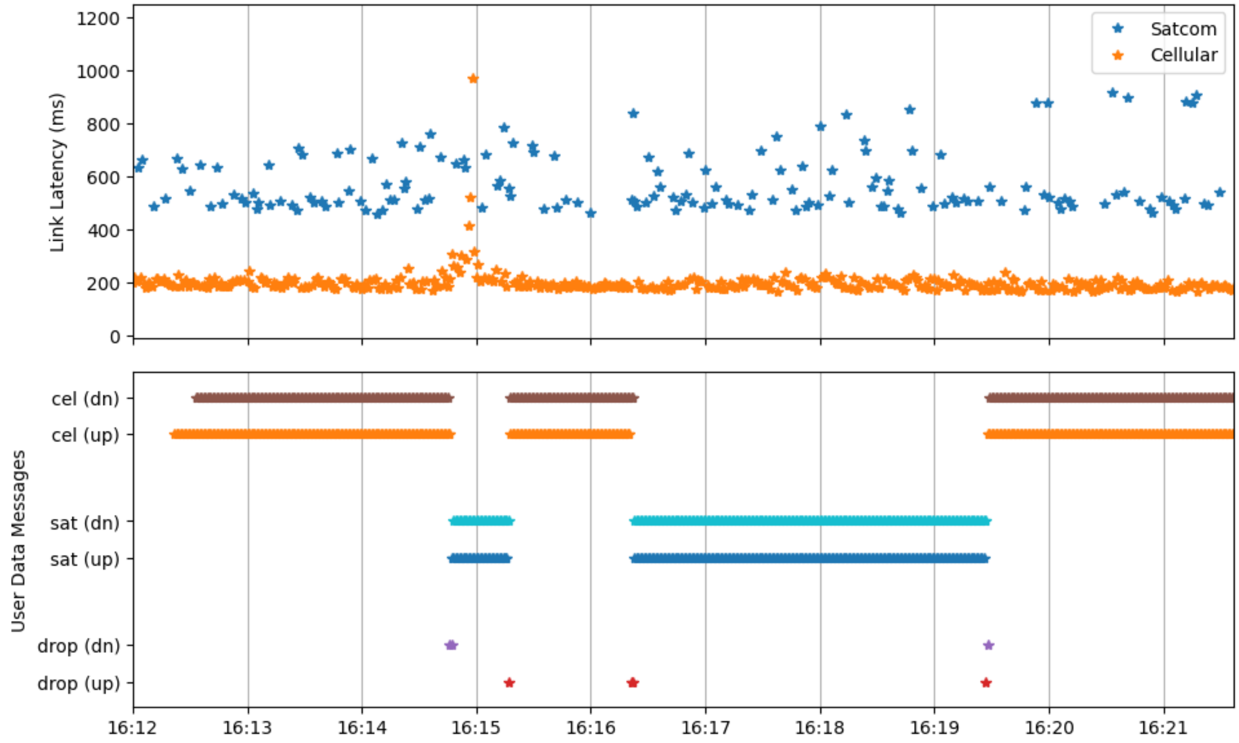


Figure 5-24. Link Latency and User Data Message Stream Path, Walking Path Flight 2

5.1.9 Target B – Walking Path – Flight 3-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	3	24 Aug 2023	4:41 CDT	5:00 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	4:41 CS Status Secure No/No-2. good. then UA same good. 4:41 UA send n=1 not recd - good. 4:41 CS Status 1/2 both links up nominal. 4:42 UA Status 1/2 both links up nominal. 4:42 UA Secure Start - up on LTE - good. 4:42 CS Status Secure - Yes/Yes-2 good then UA same Yes/Yes-2 good. 4:43 CS start sending continuous user data stream. then UA good.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:46 ARMING / SPINNING / TAKEOFF - Flight #3 4:46 UA Send n=1, recd id=2, then CS recd id=4
TP_CM_004B	User Data exchanges > MTU	**PASS**	4:47 Taking Picture Flight3-LTE, Downloading - good.
TP_CM_009	Link switchover < TET	**PASS**	4:48 CS & UA Status 1/2 both links up - good 4:49 Switchover from LTE to Satcom. 4:49 UA status secure Yes/Yes-1, then CS same good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:49 UA send n=1 , recd id=6
TP_CM_009	Link switchover < TET	**PASS**	4:49 Noticed auto-switchover from Satcom to LTE. 4:50 Switchover from LTE to Satcom manual. good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004B	User Data exchanges > MTU	**PASS**	4:57 taking picture over satcom. and downloaded.
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:58 Send n=1 recd id=8, then CS id=4 recd good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	4:58/9 LANDED / End of flight #3 4:59 Send n=1 recd id=10.
TP_CM_011	Control / User Plane Termination	**PASS**	5:00 CS Status Secure Yes/Yes-1, then UA same - good. 5:00 UA Secure stop. 5:00 CS Status secure No/No-1 - good. then UA same good. 5:00 UA Send n=1 not recd good.

Detailed Results:

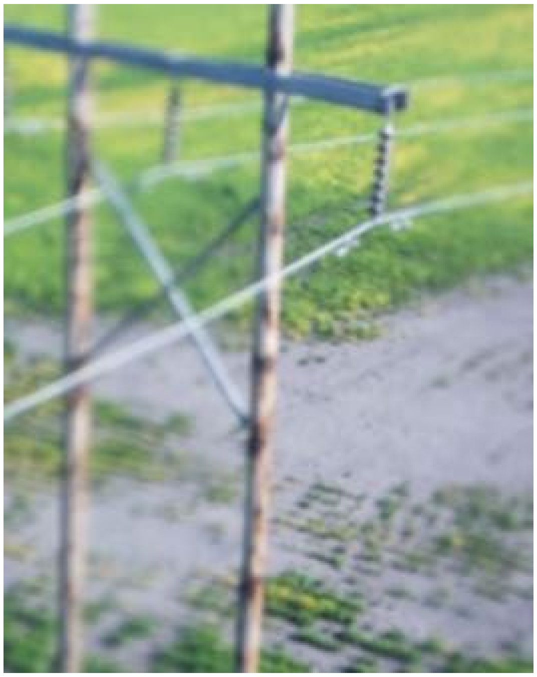


Figure 5-25. Flight 3, picture on LTE

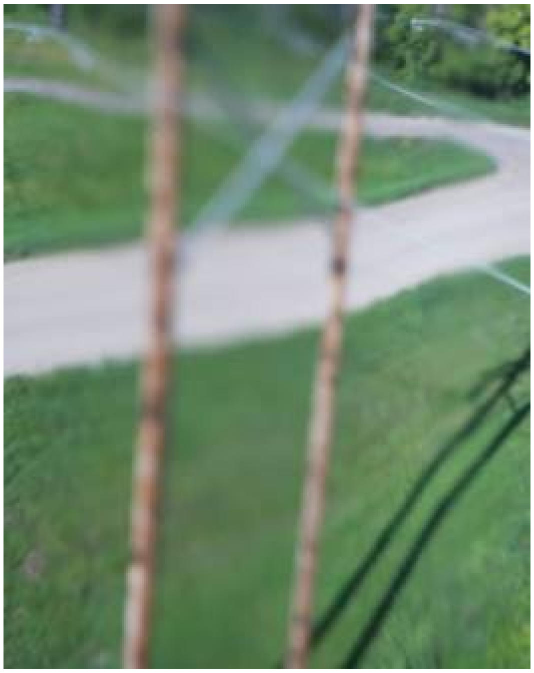


Figure 5-26. Flight 4, picture on SATCOM

Table 5-9. Commanded Link Switchover Times for Walking Path Flight 3

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	3	UA	24-Aug	4:49	satcom	LTE	465	5000	Y
Walking Path	3	CS	24-Aug	4:49	satcom	LTE	950	5000	Y
Walking Path	3	UA	24-Aug	4:50	LTE	satcom	1862	5000	Y
Walking Path	3	CS	24-Aug	4:50	LTE	satcom	1888	5000	Y

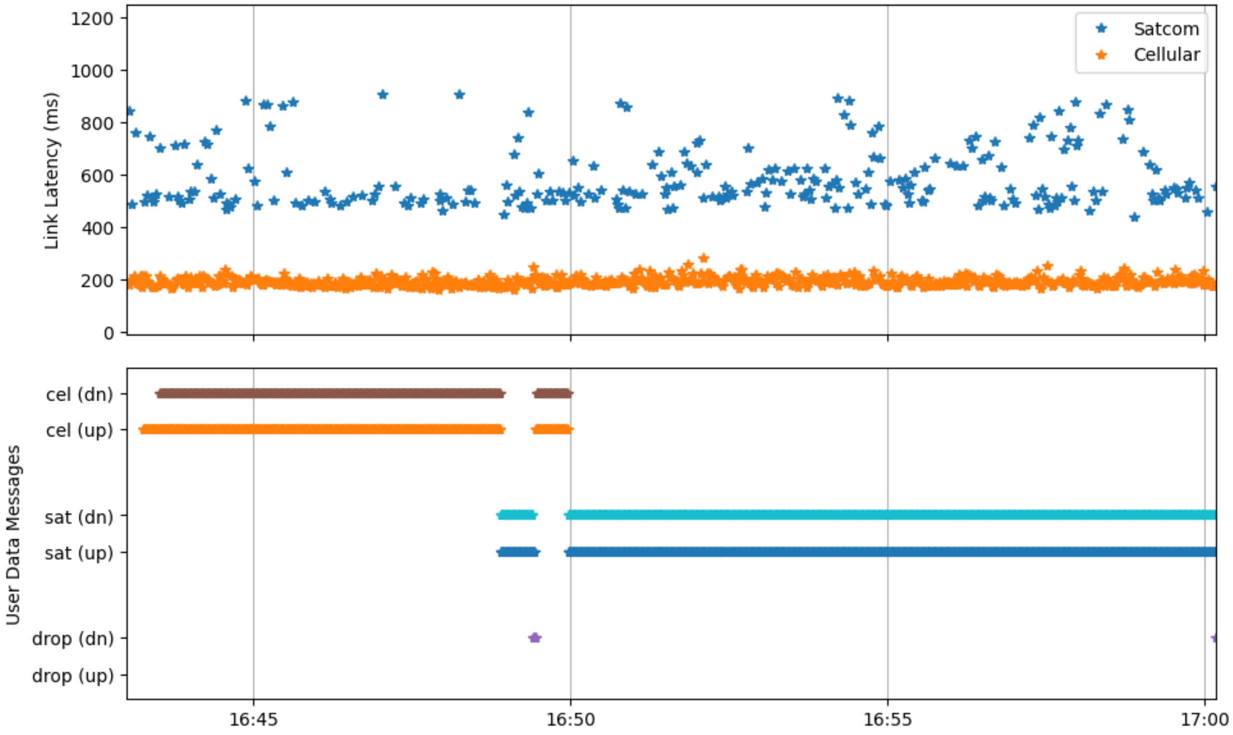


Figure 5-27. Link Latency and User Data Message Stream Path, Walking Path Flight 3

5.1.10 Target B – Walking Path – Flight 4-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	4	24 Aug 2023	5:13 CDT	5:33 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	5:13 CS Status Secure No/No-2, then UA No/No-2 good. 5:13 UA Send n=1 not recd. good 5:13 CS Status 1/2 both links up nominal - good. 5:14 CS Status 1/2 both links up nominal - good. 5:14 UA Secure Start - good link up on LTE. 5:14 CS Status Secure Yes/Yes-2, then UA same good. 5:14 CS Start sending user data stream. 5:15 UA Start sending user data stream. good.
TP_CM_004A	User Data exchanges < MTU	PASS	5:16 ARMING / SPINNING / TAKEOFF Flight #4 5:16 send n=1 recd id=4, then CS recd id=2.
TP_CM_004B	User Data exchanges > MTU	PASS	5:17 Taking Picture Day4 Flight4 LTE 5:18 Downloaded Picture over LTE.
TP_CM_009	Link switchover < TET	PASS	5:18 CS Status 1/2 both links up nominal , then UA nominal good. 5:18 Switchover manual from LTE to Satcom good. 5:18 UA Status Secure Yes/Yes-1 good. 5:19 CS Status Secure Yes/Yes-1 good.
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	5:19 UA Send n=1, recd id=6
TP_CM_004B	User Data exchanges > MTU	PASS	5:28 Taking Picture Day4 Flight4-Satcom. 5:29 Downloading Picture over Satcom... good.
TP_CM_009	Link switchover < TET	PASS	5:29 CS Status 1/2 both links up good. Noticed LTE Went up and down 5:30 UA Status 1/2 both links up nominal. good. 5:30 UA Switchover from Satcom to LTE 5:30 UA Status Secure Yes/Yes-2 then on CS Yes/Yes-2. good.
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	5:30 cleared to return to land. 5:31 UA Send n=1 recd id=8, then CS recd id=4.
TP_CM_011	Control / User Plane Termination	PASS	5:32 LANDED / ON GROUND / STOPPED 5:32 CS Status Secure Yes/Yes-2 good. then on UA good. 5:32 UA Secure Stop. 5:32/3 CS Status Secure No/No-2 then UA No/No-2 good. 5:33 UA Send n=1 not recd good.

Detailed Results:

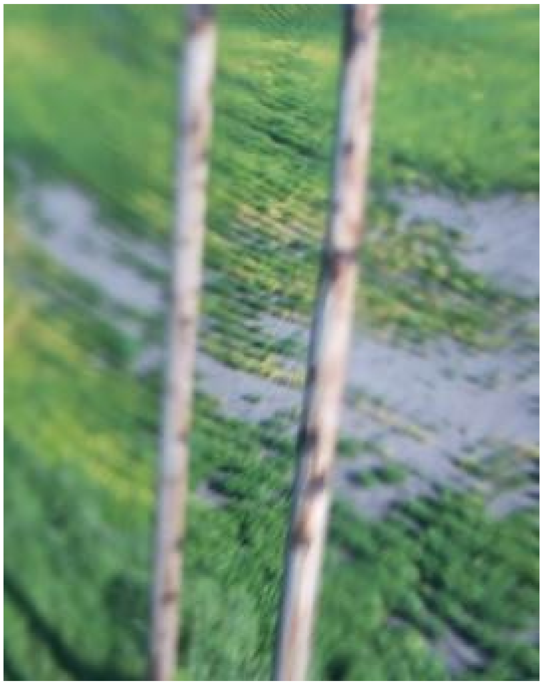


Figure 5-28. Flight 4, picture on LTE

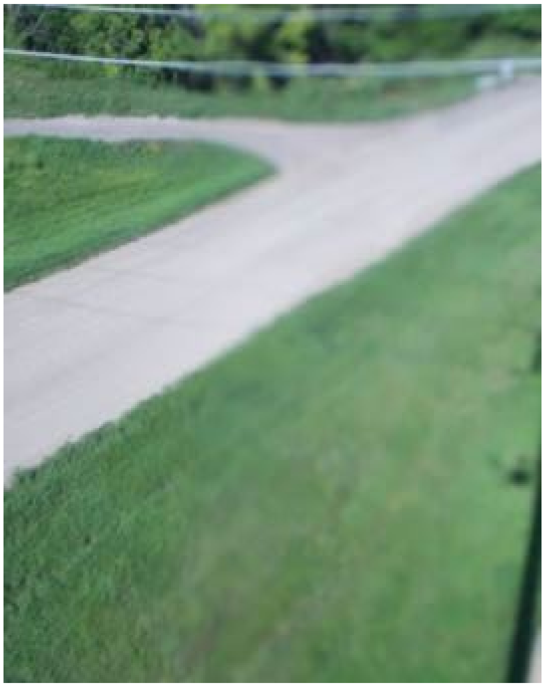


Figure 5-29. Flight 4, picture on SATCOM

Table 5-10. Commanded Link Switchover Times for Walking Path Flight 4

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	4	UA	24-Aug	5:18	LTE	satcom	1189	5000	Y
Walking Path	4	CS	24-Aug	5:18	LTE	satcom	1637	5000	Y
Walking Path	4	UA	24-Aug	5:30	satcom	LTE	1039	5000	Y
Walking Path	4	CS	24-Aug	5:30	satcom	LTE	368	5000	Y

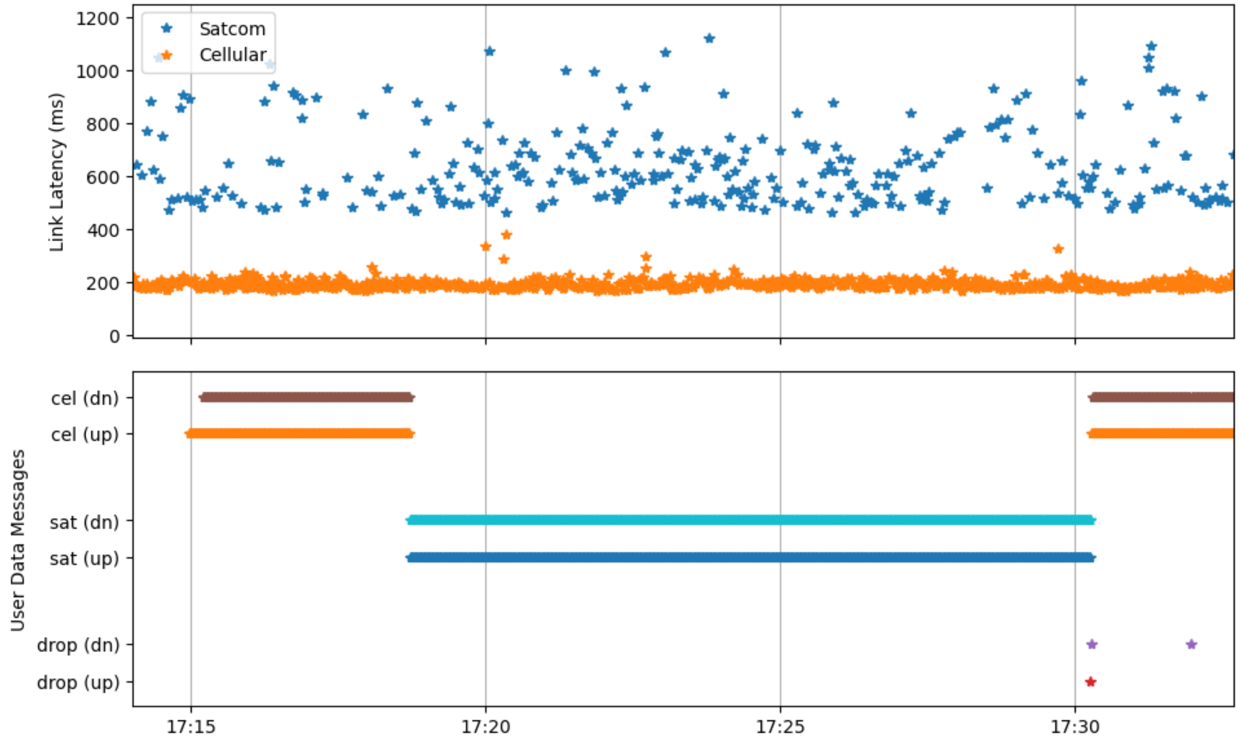


Figure 5-30. Link Latency and User Data Message Stream Path, Walking Path Flight 4

5.1.11 Target B – Walking Path – Flight 5-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	5	24 Aug 2023	5:43 CDT	6:04 CDT

General Test Observations: The UA and CS DTSRs got out of sync during this flight, but the CS operator was able to restart the DTSRs at 6:00 CDT, and the system recovered in time to continue testing without negative impact to the test sequence.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	5:43 CS Status Secure No/No-2, then UA No/No-2 good. 5:43 UA Send n=1 not recd good. 5:44 CS Status 1/2 both links up nominal. good. then UA. same good. 5:44 UA Secure Start... good over LTE. 5:44 CS Status Secure Yes/Yes-2, then UA Yes/Yes-2 good. 5:45 CS Start sending continuous user data stream. then UA. good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	5:46 ARMING / SPINNING / TAKEOFF Flight 5 5:46 Send n=1 recd id=4, then CS recd id=2.
TP_CM_004B	User Data exchanges > MTU	**PASS**	5:48 Taking Picture Day4 Flight5 LTE. good. 5:48 Downloaded Picture over LTE.
TP_CM_009	Link switchover < TET	**PASS**	5:48 NOTED auto-switchover. multiple times... 5:49 UA Status Secure Yes/Yes-1, then CS Status Secure Yes/Yes-1. good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A.	User Data exchanges < MTU	**PASS**	5:50 UA Send n=1 recd id=6.
TP_CM_004B	User Data exchanges > MTU	**PASS**	5:57 Taking Picture day4Flight5 over Satcom. 5:59 ISSUE/ERROR Noticed UA was on Satcom and CS was on LTE. lost secure connection. 6:00 restarting DTSRs. 6:00 Switchover from LTE to Satcom manual good. 6:00 Taking Picture over Satcom... good. 6:01 Downloading Picture over Satcom... good.
TP_CM_009	Link switchover < TET	**PASS**	6:01 CS Status 1/2 both links up. then UA same good. 6:02 Switchover to LTE. 6:02 Status Secure Yes/Yes-2 then CS Yes/Yes-2.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:03 send n=1 id=10, then CS id=4.
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:03 LANDED 6:03 send n=1 id=12.
TP_CM_011	Control / User Plane Termination	**PASS**	6:03 Status Secure Yes/Yes-2 on both.s 6:04 Secure Stop. 6:04 CS Status Secure No/No-2 , then UA No/No-2 good. 6:04 UA send n=1 not recd. good.

Detailed Results:

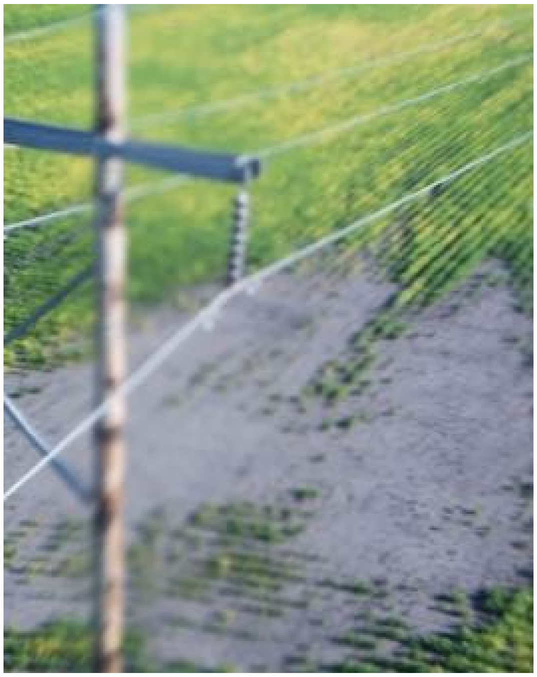


Figure 5-31. Flight 5, picture on LTE

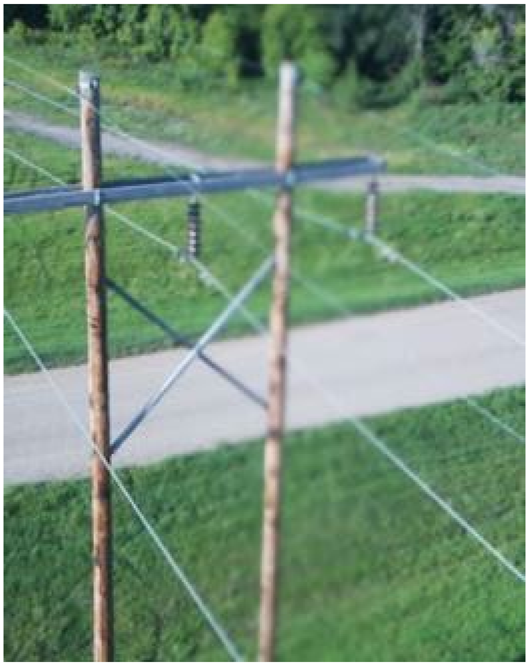


Figure 5-32. Flight 5, picture on SATCOM

Table 5-11. Commanded Link Switchover Times for Walking Path Flight 5

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	5	UA	24-Aug	6:00	LTE	satcom	1258	5000	Y
Walking Path	5	CS	24-Aug	6:00	LTE	satcom	1475	5000	Y
Walking Path	5	UA	24-Aug	6:02	LTE	satcom	1514	5000	Y
Walking Path	5	CS	24-Aug	6:02	LTE	satcom	427	5000	Y

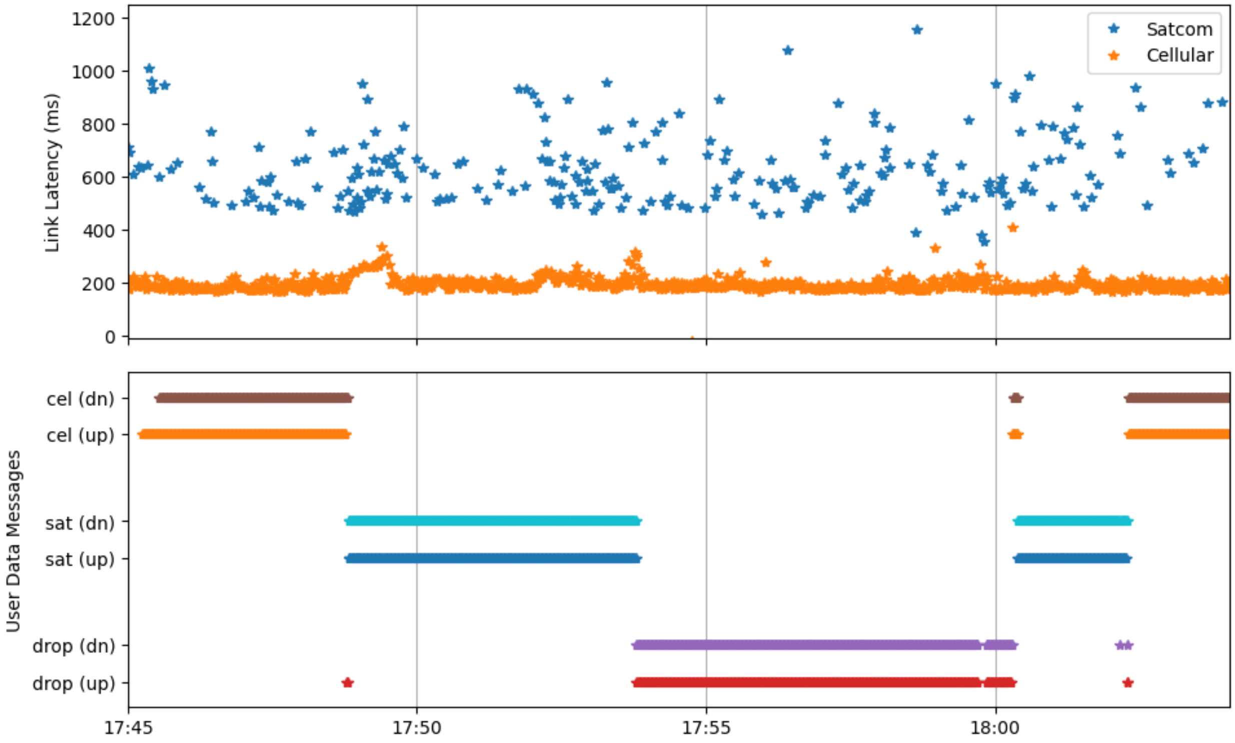


Figure 5-33. Link Latency and User Data Message Stream Path, Walking Path Flight 5

5.1.12 Target B – Walking Path – Flight 6-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target B (Walking Path), Nominal tests, with encryption	6	DD MMM 2023	6:13 CDT	6:33 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	6:13 CS Status Secure No/No-2, then UA same good. 6:14 UA N=1 not recd. good. 6:14 CS Status 1/2 both links up nominal , then UA same good. 6:14 UA Secure Start... link up on LTE. good. 6:14 CS Status Secure Yes/Yes-2. good. then UA. Yes/Yes-2 good. 6:15 CS Start sending data stream. then UA. good.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:16/7 ARMING / SPINNING / TAKEOFF Flight #6 6:17/8 UA send n=1, recd id=4, then CS id=2 good.
TP_CM_004B	User Data exchanges > MTU	**PASS**	6:18 Taking Picture good. 6:19 Downloading Picture over LTE. good.
TP_CM_009	Link switchover < TET	**PASS**	6:19 CS Status 1/2 both link up good, then UA same good. 6:20 UA Switchover from LTE to Satcom good. 6:20 UA Status Secure Yes/Yes-1 good. then CS Yes/Yes-1 good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:27 UA Send n=1, recd id=6 over satcom
TP_CM_004B	User Data exchanges > MTU	**PASS**	6:28 Taking Picture Day4 Flight 6 Satcom. good. 6:29 Downloading picture over satcom. good.
TP_CM_009	Link switchover < TET	**PASS**	6:29 CS Status 1/2 both links up nominal. good. then UA same - good. 6:30 UA Switchover from Satcom to LTE - good. 6:30 UA Status Secure Yes/Yes-2, then on CS same, good.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:30 UA Send n=1, recd, id=8. 6:30/1 UA Send n=1, id=10, then CS recd id=4. good.
TP_CM_004A	User Data exchanges < MTU	**PASS**	6:31/2 LANDED 6:32 send n=1, recd id=12, id=6
TP_CM_011	Control / User Plane Termination	**PASS**	6:32 send n=1, recd id=12, id=6 6:32 CS Status secure Yes/Yes-2, then ua good. 6:32/3 UA Secure Stop. 6:33 CS Status Secure No/No-2, then UA, same good. 6:33 UA send n=1, not recd good.

Detailed Results:

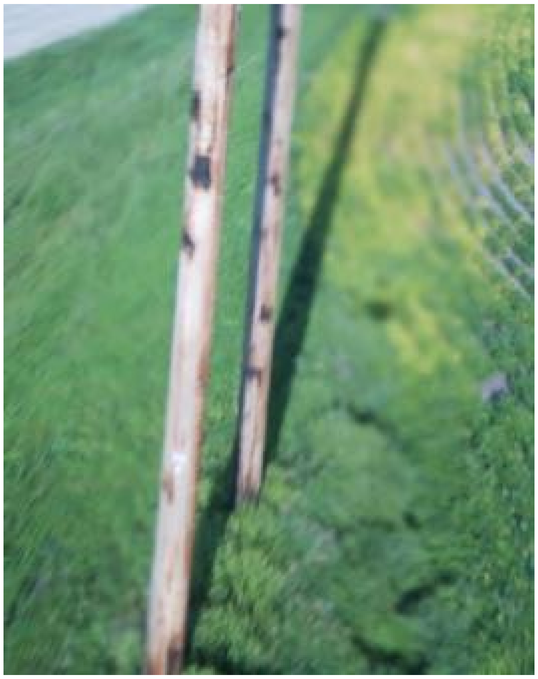


Figure 5-34. Flight 6, picture on LTE

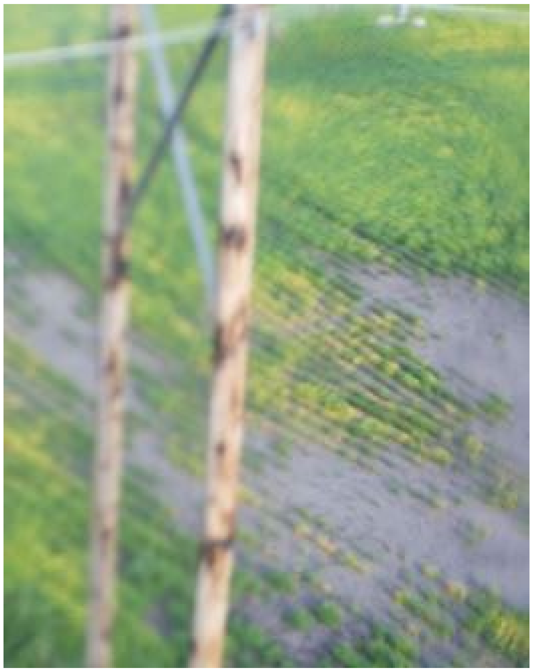


Figure 5-35. Flight 6, picture on SATCOM

Table 5-12. Commanded Link Switchover Times for Walking Path Flight 6

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Walking Path	6	UA	24-Aug	6:20	LTE	satcom	1153	5000	Y
Walking Path	6	CS	24-Aug	6:20	LTE	satcom	2043	5000	Y
Walking Path	6	UA	24-Aug	6:30	satcom	LTE	1272	5000	Y
Walking Path	6	CS	24-Aug	6:30	satcom	LTE	418	5000	Y

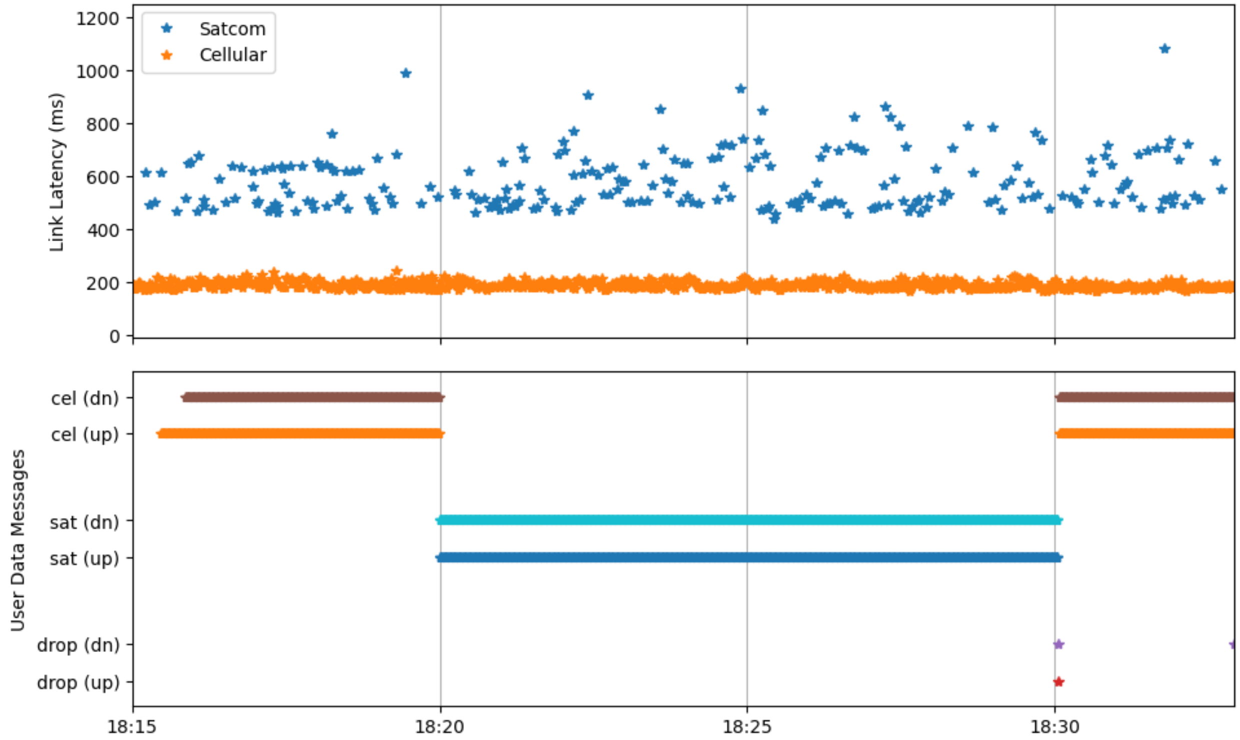


Figure 5-36. Link Latency and User Data Message Stream Path, Walking Path Flight 6

5.1.13 Target C – Building – Flight 1-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	1	23 Aug 2023	1:06 CDT	1:20 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	**PASS**	1:06 CS: Status Secure: No/No-2 1:06 UA: Status Secure: No/No-2 1:07 UA: Send N=1 1:07 verifying UA-main-sniffer. Verified success. 1:07 verifying CS-main-sniffer. Verified Success. 1:08 CS Status 1/2. Both links up. 1:08 UA Status 1/2. Both links up. 1:08 UA: SECURE START. Successful on LTE (link-2). 1:09 CS: Status Secure: Yes/Yes-2 (LTE) 1:10 UA: Status Secure Yes/Yes-2 (LTE). 1:10 CS: Started sending user data stream. 1:10 UA: Started sending user data stream.
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:16 Sent N=1 on both sides.
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:18 Took Picture Day3-Flight 1. Success. 1:18 Downloading Picture on LTE. Success.
TP_CM_009	Link switchover < TET	**PASS**	1:19 CS Status 1/2 Both links UP. latency nominal. 1:19 UA Status 1/2 Both inks UP. latency nominal. 1:19 UA SWITCHOVER TO 1: Successful switchover from LTE to SATCOM. 1:20 UA status Secure: Both Yes/Yes-1 (Satcom). 1:20 CS Status secure: Both Yes/Yes-1 (Satcom).
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004B	User Data exchanges > MTU	**PASS**	1:21 Taking Picture Day3-flight1-Satcom. Successful. 1:21 Downloading Picture over Satcom. Successful.
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:22 UA: Send N=1, received by CS UDMD.
TP_CM_009	Link switchover < TET	**PASS**	1:23 CS: Status 1/2 both links up. 1:23 UA: Status 1/2 both links up. 1:23 UA SWITCHOVER to 2. from Satcom to LTE. Successful. 1:23 UA Status Secure Yes/Yes-2 (LTE) 1:24 CS Status Secure Yes/Yes-2
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:25 UA Send n=1 1:25 CS Send n=1
TP_CM_004A	User Data exchanges < MTU	**PASS**	1:25 LANDED Stopped blades. drone on ground. 1:25/26 UA: Send n=1

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	PASS	Noted there was an autoswitchover. 1:26 CS. Status Secure. Yes/Yes-1 1:26 UA. Status Secure Yes/Yes-1 1:27 UA. Secure Stop. 1:27 CS Status Secure No/No-1 1:27 UA Status Secure No/No-1. 1:27 UA. Send n=1 1:28 UA Send n=1. Verified on UA main sniffer it wasn't sent. 1:29 Verified on CS message wasn't received.

Detailed Results:

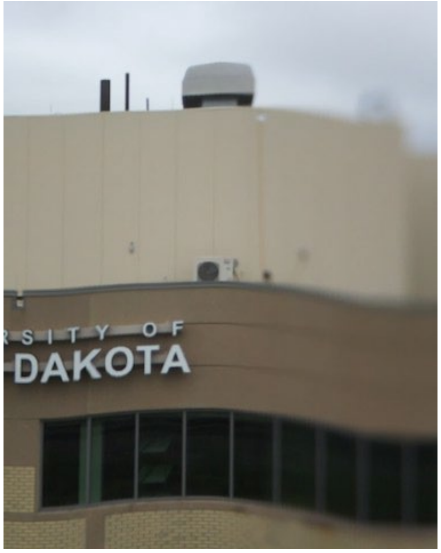


Figure 5-37. Flight 1, picture on LTE

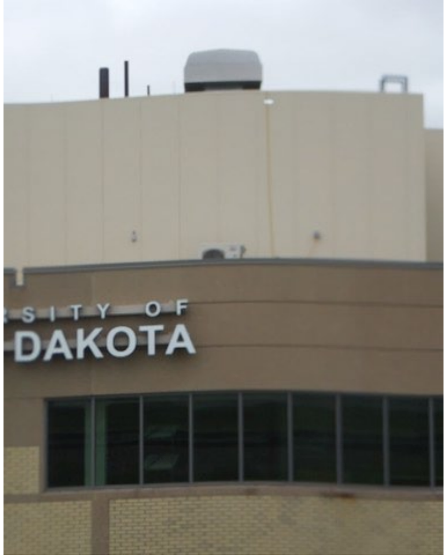


Figure 5-38. Flight 1, picture on SATCOM

Table 5-13. Commanded Link Switchover Times for Building Flight 1

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Building	1	UA	23-Aug	1:19	LTE	satcom	1706	5000	Y
Building	1	CS	23-Aug	1:19	LTE	satcom	1276	5000	Y
Building	1	UA	23-Aug	1:23	satcom	LTE	1141	5000	Y
Building	1	CS	23-Aug	1:23	satcom	LTE	400	5000	Y

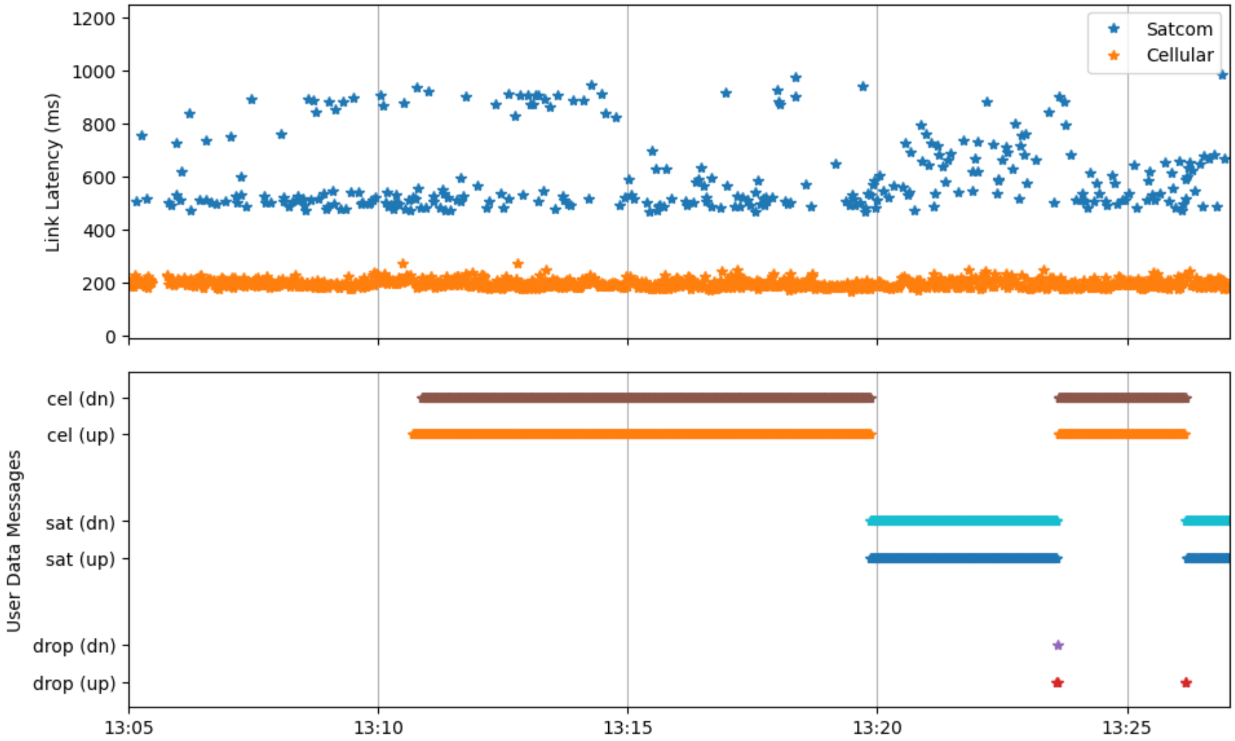


Figure 5-39. Link Latency and User Data Message Stream Path, Building Flight 1

5.1.14 Target C – Building – Flight 2-of-6 (Nominal)

Result = PARTIAL: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET. The first six procedures in this test sequence passed, but the second half of the sequence failed.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	2	23 Aug 2023	1:52 CDT	2:09 CDT

General Test Observations: The UA and CS DTSRs encountered an error around 2:02, and all test procedures after that failed. We suspect the DTSRs got out of sync and did not recover.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	🟩 PASS	1:52 CS Status Secure. No/No-2 1:52 UA Status Secure No/No-2 1:53 UA Send n=1 1:53 verifying on UA main sniffer... passed 1:55 CS Status 1/2 both links UP good latencies. 1:55 UA Status 1/2 both links up good latencies. 1:55/56 UA Secure Start. 1:56 CS Status Secure: Yes/Yes-2 (LTE) 1:56 UA Status Secure: Yes/Yes-2 (LTE). 1:57 CS started sending data stream 1:57 UA Started sending data stream. 1:57 Ready for takeoff...
TP_CM_004A	User Data exchanges < MTU	🟩 PASS	1:58 ARMING / SPINNING / TAKEOFF Flight #2 1:58 UA & CS. Sending n=1
TP_CM_004B	User Data exchanges > MTU	🟩 PASS	1:59 Taking picture Day3flight2- LTE. Still on LTE Secure Session. 1:59 Downloading Picture.
TP_CM_009	Link switchover < TET	🟩 PASS	2:00 CS Status 1/2 both links up. 2:00 UA Status 1/2 both links UP. 2:00 UA: Switchover Switch 1. from LTE to SATCOM. good. 2:00 UA Status Secure. Yes/Yes-1. (satcom). 2:00 CS Status Secure. Yes/Yes-1.
TP_CM_007	Control message exchanges	🟩 PASS	
TP_CM_004B	User Data exchanges > MTU	🟩 PASS	2:01 Taking Picture on satcom, Day3flight2 satcom. 2:01 Downloading Picture on Satcom. 2:02 Download complete over satcom. At 2:02, we lost the user data stream.
TP_CM_004A	User Data exchanges < MTU	🟥 FAIL	2:02 UA Send N=1 ISSUE/ERROR it wasn't received 2:03 UA Send N=1 ISSUE/ERROR not received. 2:03 CS Send n=1 ISSUE/ERROR not received.
TP_CM_009	Link switchover < TET	🟥 FAIL	2:03 CS Status 1/2 Both links up 2:04 UA Status 1/2 Both links up. 2:04 SWITCHOVER Switch 2. Still on "satcom" Switchover Failed. ISSUE/ERROR DTSR SESSION IS GONE. 2:05 UA Status Secure. Yes/Yes-2 (LTE). 2:05 CS Status Secure. Yes/Yes-1 (Satcom). ISSUE/ERROR DTSR connection is lost??>...
TP_CM_007	Control message exchanges	🟥 FAIL	

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	FAIL	2:06 UA Send n=1 2:06 CS Send n=1 2:07 approaching to land... 2:07 LANDED Stopped. Drone now on ground. 2:07 UA Send n=1 2:07 CS Status Secure. Yes/Yes-1. 2:07 UA Status Secure Yes/Yes-1. 2:08 UA Secure Stop. 2:08 CS Secure Stop. 2:08 CS Status Secure. No/No-1 2:09 UA Status Secure. No/No-1. 2:09 UA Send n=1
TP_CM_011	Control / User Plane Termination	FAIL	

Detailed Results:

Unfortunately, the DTSR logs do not cover this flight in its entirety as there is a gap of about 24 minutes from 18:34 to 19:10 GMT. As a result, we cannot explain with certainty what caused the loss of the user data stream at 2:02 and the DTSRs to become disconnected at 2:05 CDT. From the logs and sniffer files that do exist, the behavior is consistent with the UA DSTR switching links and getting out of sync with the CS DTSR. Essentially, the DTSRs were tunneling their traffic through different links and could not communicate with one another this way.

The first link switchover from LTE to SATCOM was successful, but the exact times for the switchovers are recoded in the DTSR logs which are incomplete. We did not observe any warnings that TET was exceeded.

This flight on August 23rd was our second test flight to execute, so we were unfamiliar with the symptoms of this software error. As the problem re-occurred in subsequent flights, we were able to recognize the pattern and recover more efficiently by immediately re-starting the DTSRs.

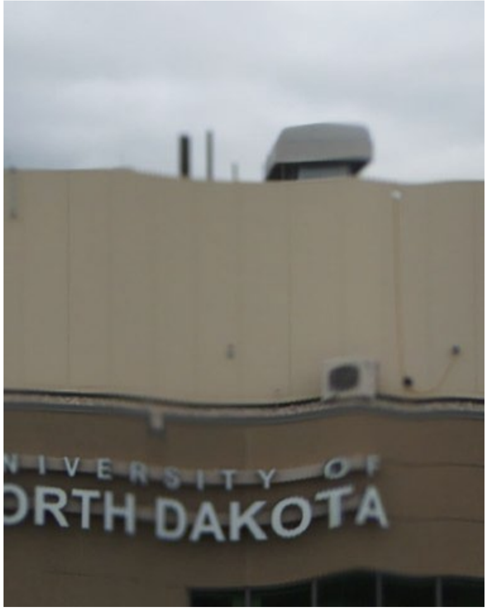


Figure 5-40. Building flight 2, picture sent on LTE

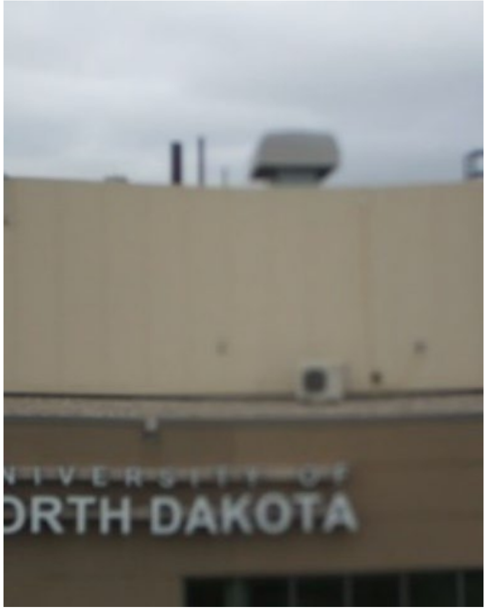


Figure 5-41. Building flight 2, sent on SATCOM

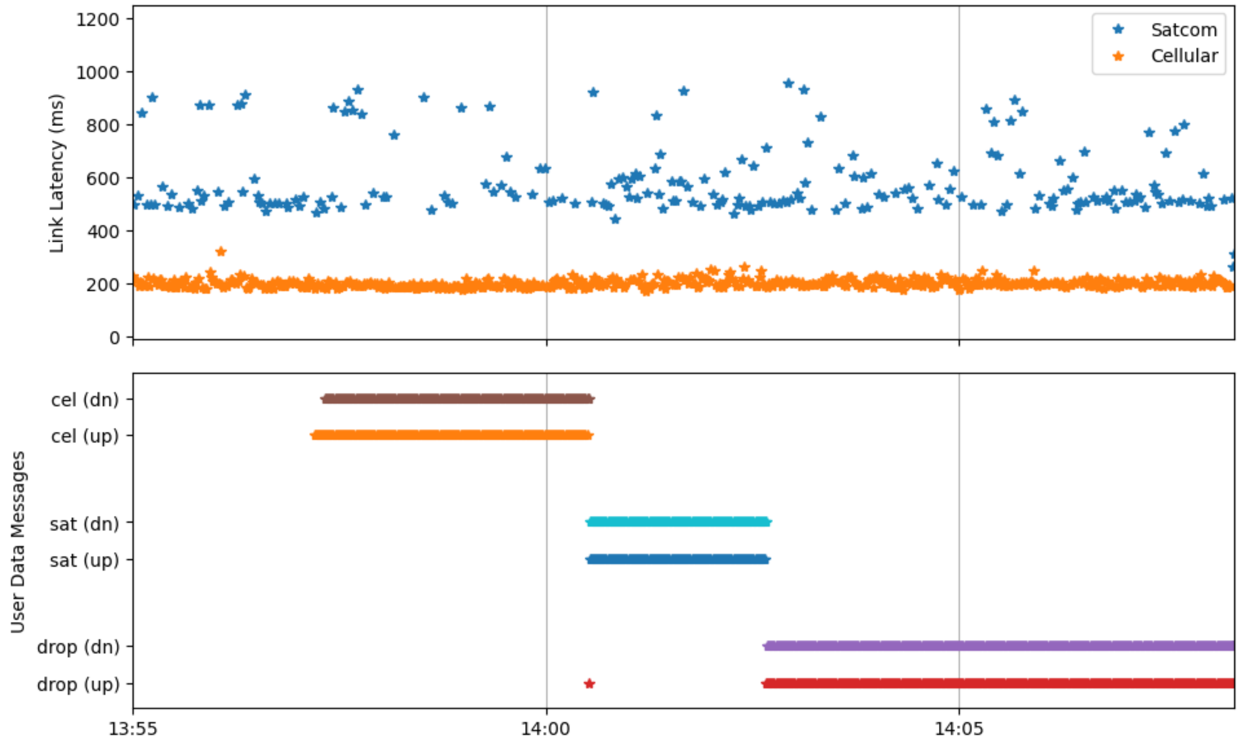


Figure 5-42. Link Latency and User Data Message Stream Path, Building Flight 2

5.1.15 Target C – Building – Flight 3-of-6 (Nominal)

Result = PARTIAL: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET. Some procedures in this test sequence passed while others failed or could not be attempted.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	3	23 Aug 2023	2 :26 CDT	2:48 CDT

General Test Observations: During the TP_CM_004B procedure, while attempting to send the first image over LTE, we lost the connection over the secure user plane. We realized we had three data streams from the CS, resulting in bandwidth issues. Troubleshooting this problem took 12 minutes which prevented the testing of other procedures on this flight, as the drone's battery life could not sustain flight for longer.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	2:26 Started CS DTSR. 2:26 Started UA DTSR. LMSF Connected. 2:27 CS Status Secure No/No-2 2:27 UA Status Secure No/No-2 2:27 UA Send n=1 2:27 verifying... main-sniffer. good. 2:28 UA SECURE START. Good, LTE SECURE. 2:29 CS Status Secure Yes/Yes-2 2:29 UA Status Secure Yes/Yes-2 2:30 CS Starting continuous data stream 2:30 UA starting continuous data stream. verified on Wireshark.
TP_CM_004A	User Data exchanges < MTU	PASS	2:31 ARMING / SPINNING / TAKEOFF 2:31 UA Send n=1 2:31 CS Send n=1
TP_CM_004B	User Data exchanges > MTU	FAIL	2:33 Taking Picture Day3-Flight3 over LTE. 2:35 ISSUE/ERROR acquire returned Port 22 connection timed out. 2:35 Re sending command to take picture. Python error. 2:36 Re sending command to take picture... 2:37 UA Send N=1, not received. 2:37 CS Send N=1, not received. 2:38 CS Status 1/2 both links up. 2:38 UA Status 1/2 both links up. 2:38 ISSUE/ERROR CONNECTION LOST OVER USER PLANE (Secure). 2:39 stopped user data. Realized we had 3 CS Data streams running. 2:40 stopped all data streams sending from the CS. 2:40/1 re-issuing command to take picture.
TP_CM_009	Link switchover < TET	NONE	
TP_CM_007	Control message exchanges	NONE	
TP_CM_004B	User Data exchanges > MTU	PASS	2:43 Restarting DTSR's. 2:43 Both DTSR's restarted and running. 2:44 UA Secure Start. successful. 2:44 Capturing image failed, image name already exists. 2:45 Taking image day3flight2-1 with new name. 2:45 Downloaded picture over LTE, successful
TP_CM_009	Link switchover < TET	NONE	
TP_CM_004A	User Data exchanges < MTU	PASS	2:45 Send N=1 from CS. 2:45/6 UA Send n=1 2:46 Approaching to Land. 2:46 LANDED / ON Ground stopped blades.

Procedure	Description	Result	Notes
TP_CM_011	Control / User Plane Termination	NONE	

Detailed Results:

The logs from this flight indicate that the DTSRs got out of sync due to the same software issue as previous flights. After restarting the DTSRs while the aircraft was in the air, the system recovered.

Figure 5-43. Building flight 3, image sent on LTE

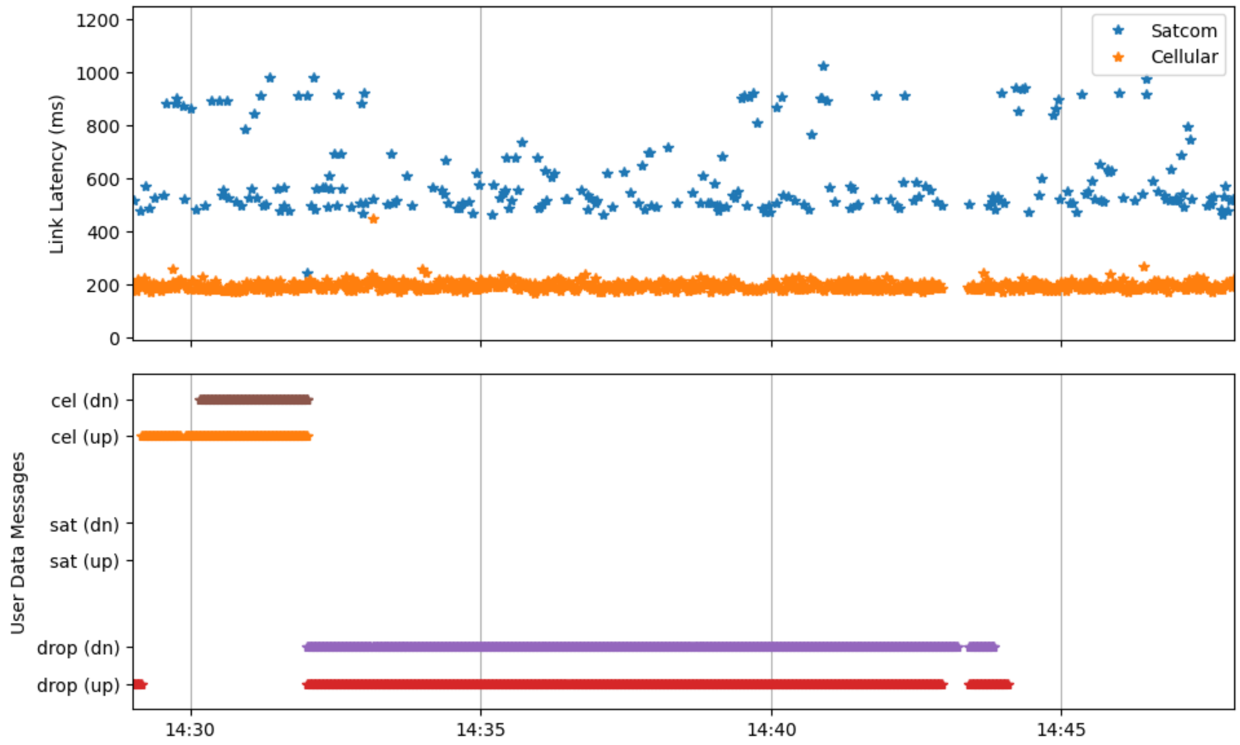


Figure 5-44. Link Latency and User Data Message Stream Path, Building Flight 3

5.1.16 Target C – Building – Flight 4-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	4	23 Aug 2023	3:02 CDT	3:17 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	3:02 CS Status Secure No/No-2 3:02 UA Status Secure No/No-2 3:03 UA Send N=1 3:03 verifying on ua main sniffer. PCAP LOG 23-14.48.51.PCAP 3:04 UA Secure START. good Secure on LTE. 3:05 CS Status Secure Yes/Yes-2 3:05 UA Status Secure Yes/Yes-2 3:05 Started sending data stream from CS. 3:05 Started sending data stream from UA.

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:06 ARMING / SPINNING / TAKEOFF 3:07 Flight #4 3:07 Send N=1 from both, both good
TP_CM_004B	User Data exchanges > MTU	**PASS**	3:08 taking picture day3-flight4-LTE 3:08 Downloading picture over LTE
TP_CM_009	Link switchover < TET	**PASS**	3:09 CS Status 1/2: both links up. normal latencies. 3:09 UA Status 1/2: both links up. normal latencies. 3:09 UA SWITCHOVER Switch-1 from LTE to Satcom. good. 3:10 UA status secure. Yes/Yes-1. 3:10 CS status secure. Yes/Yes-1.
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004B	User Data exchanges > MTU	**PASS**	3:10/11 Taking picture Day3-flight4-Satcom. 3:11 Downloading Picture day3-flight4-Satcom
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:12 UA Send N=1 good.
TP_CM_009	Link switchover < TET	**PASS**	3:12 CS Status 1/2 both links up. 3:12 UA Status 1/2 both links up. nominal latencies. 3:12/3 SWITCHOVER SWITCH 2 from Satcom to LTE. 3:13 UA Status Secure Yes/Yes-2 3:13 CS Status Secure Yes/Yes-2
TP_CM_007	Control message exchanges	**PASS**	
TP_CM_004A	User Data exchanges < MTU	**PASS**	3:14 approaching 3:14 UA Send N=1 3:15 CS Send N=1 both good. 3:15 LANDED / STOPPED SPINNING / ON Ground End of Flight #4 3:15 UA Send n=1
TP_CM_011	Control / User Plane Termination	**PASS**	3:16 CS Status Secure Yes/Yes-2 3:16 UA Status Secure Yes/Yes-2 3:16 UA Secure STOP (good) 3:16 CS Status Secure: No/No/No-2 3:17 UA Status Secure No/No-2 3:17 UA Send N=1

Detailed Results:

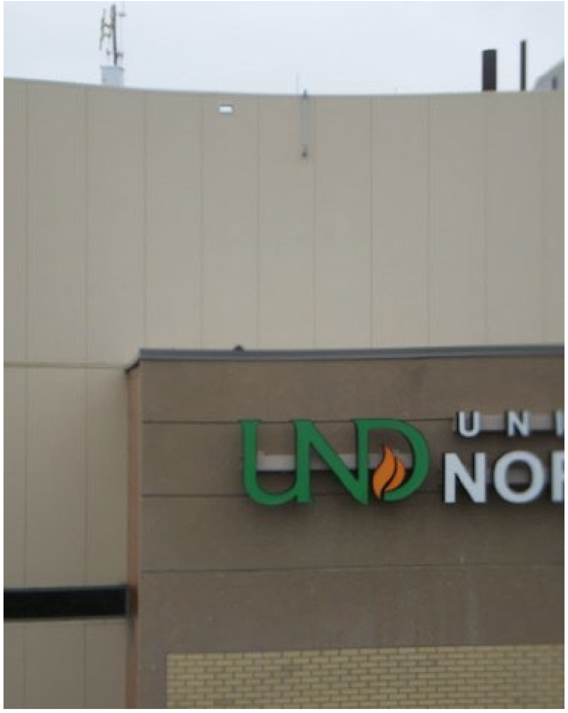


Figure 5-45. Flight 4, image sent on LTE

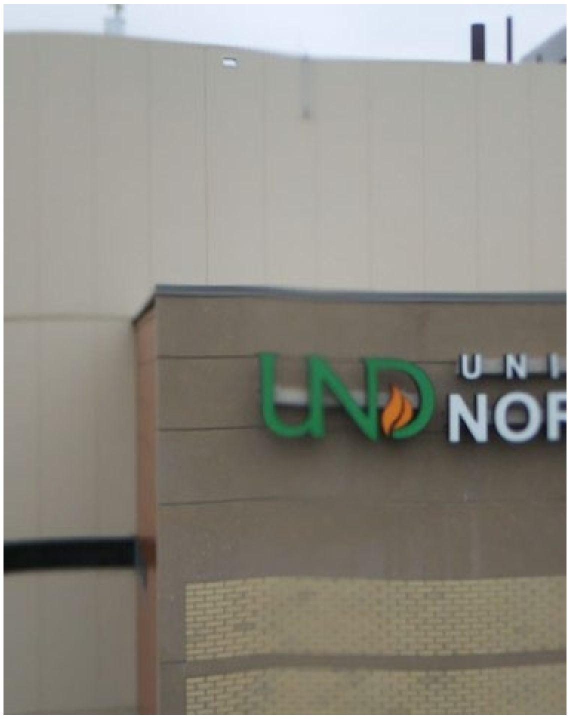


Figure 5-46. Flight 4, image sent on SATCOM

Table 5-14. Commanded Link Switchover Times for Building Flight 4

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Building	4	UA	23-Aug	3:09	LTE	satcom	1193	5000	Y
Building	4	CS	23-Aug	3:09	LTE	satcom	1214	5000	Y
Building	4	UA	23-Aug	3:12	satcom	LTE	1540	5000	Y
Building	4	CS	23-Aug	3:12	satcom	LTE	393	5000	Y

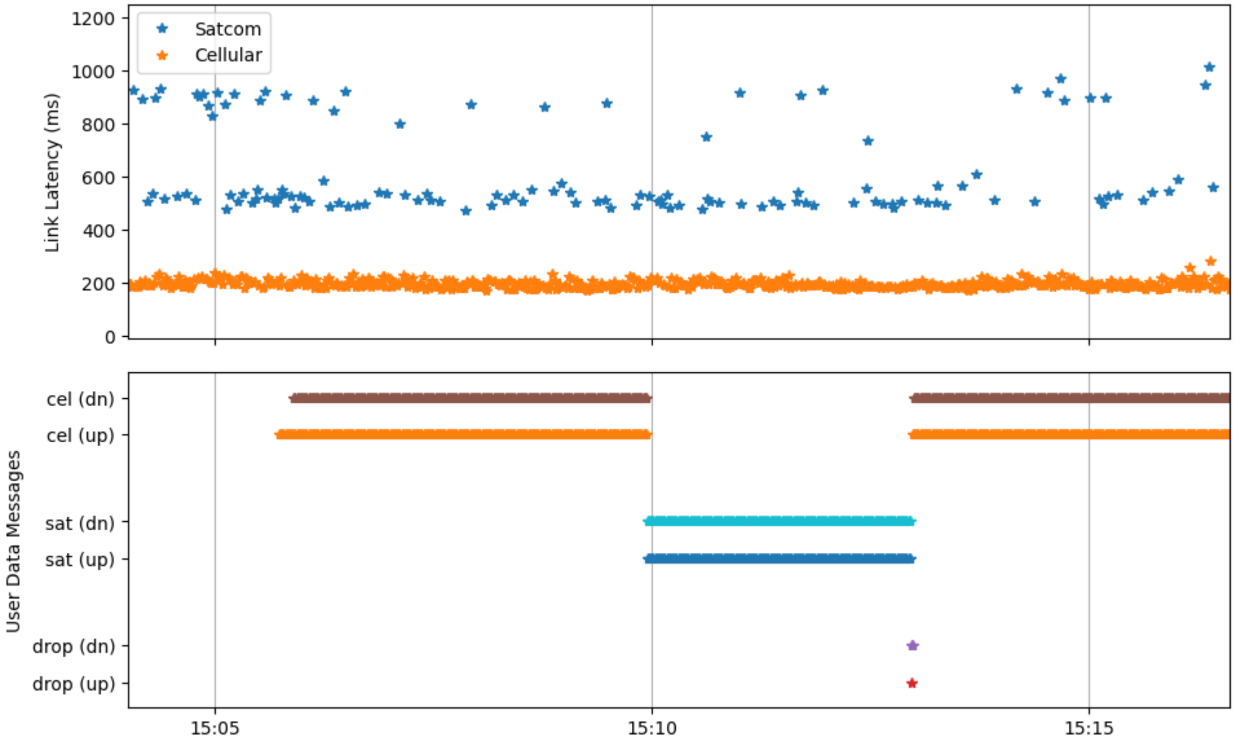


Figure 5-47. Link Latency and User Data Message Stream Path, Building Flight 4

5.1.17 Target C – Building – Flight 5-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	5	23 Aug 2023	3:26 CDT	3:46 CDT

General Test Observations: The CS operator had to restart the system at 3:41 after the links appeared to go down. The system recovered and testing resumed without causing failures.

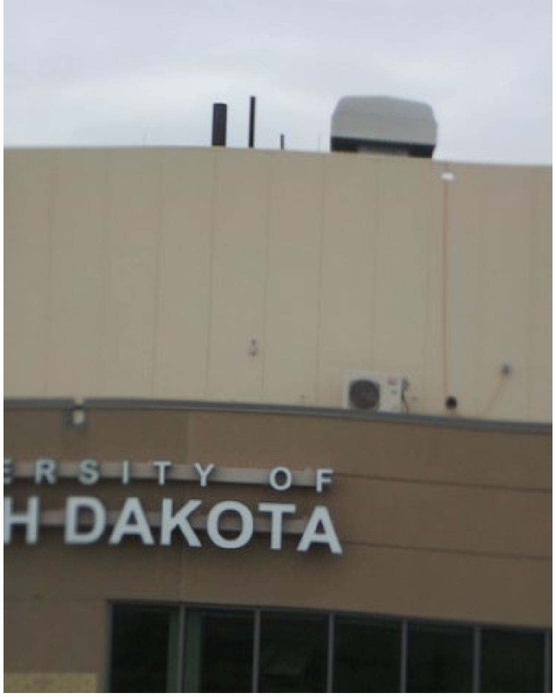
Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	3:26 CS Status Secure No/No-2 3:26 UA Status Secure No/No-2 3:27 UA Send N=1 3:27 CS Status 1/2 Both links UP. nominal latencies 3:27 UA Status 1/2 Both links UP. nominal latencies. 3:27 UA SECURE START good secure on LTE 3:28 CS Status Secure: Yes/Yes-2 3:28 UA Status Secure: Yes/Yes-2 3:28 CS Starting continuous data stream 3:30 UA Starting continuous data stream
TP_CM_004A	User Data exchanges < MTU	PASS	3:31 UA send n=1 3:31 CS Send n=1 both good.
TP_CM_004A	User Data exchanges < MTU	PASS	3:31 ARMING / SPINNING / TAKEOFF Flight #5 3:31 UA & CS n=1 both good
TP_CM_004B	User Data exchanges > MTU	PASS	3:34 taking picture day3-flight5-LTE 3:34 Downloading picture. (good)
TP_CM_009	Link switchover < TET	PASS	3:34 CS Status 1/2 both links up. nominal latencies. 3:35 UA Status 1/2 both links up. nominal. latencies 3:35 UA Switchover Switch-1 3:35 UA Status Secure Yes/Yes-1 3:35 CS status secure Yes/Yes-1
TP_CM_004A	User Data exchanges < MTU	PASS	3:35 UA Send n=1 (good)
TP_CM_004B	User Data exchanges > MTU	PASS	3:36 taking picture Day3-flight5 satcom 3:36 downloading picture day3-flight5 satcom 3:37 ISSUE/ERROR the link went down (both links went down). 3:39 stopping data stream from CS. 3:40 stopping data stream from UA. 3:40 Keep-alives indicate a failure. GUI still show good links 3:41 restarting DTSRs 3:41 UA Secure Start 3:41 Session established on LTE. 3:41 Switchover switch-1 From LTE to Satcom. 3:42 Downloading image over satcom.
TP_CM_009	Link switchover < TET	PASS	3:42 CS Status 1/2 both links Up. 3:43 UA Status 1/2 both links up. 3:43 SWITCH TO 2 Now on LTE. 3:43 CS & UA Status Secure Yes/Yes-2
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	3:44 UA Send n=1

Procedure	Description	Result	Notes
TP_CM_004A	User Data exchanges < MTU	PASS	3:45 LANDED ON GROUND 3:45 Send n=1 3:45 CS Status Secure Yes/Yes-2 3:45 UA Status Secure Yes/Yes-2
TP_CM_011	Control / User Plane Termination	PASS	3:45 UA Secure Stop 3:45 CS status secure No/No-2 3:45 UA status secure No/No-2 3:46 UA send n=1 3:46 UA Send n=1 (2nd)

Detailed Results:

During this flight, the CS operator restarted the DTSRs at 3:41 because it appeared that user data was suddenly dropped, and the operator intentionally stopped the user data stream. After the DTSRs restarted, the operator did not restart the user data stream; therefore the performance data graph does not illustrate the link recovery; however, the system was working nominally after this restart, and subsequent test procedures passed.

The software problem encountered in this test was slightly different from the other cases. Although both the UA and the CS detect the active link going down, the CS was able to switch over to link 2, but the UA did not. The UA determined both links were down at the time and was not able to decide what link to switch to. This is a limitation of the software that was corrected before the software was flown again for the UAS-C2 project.



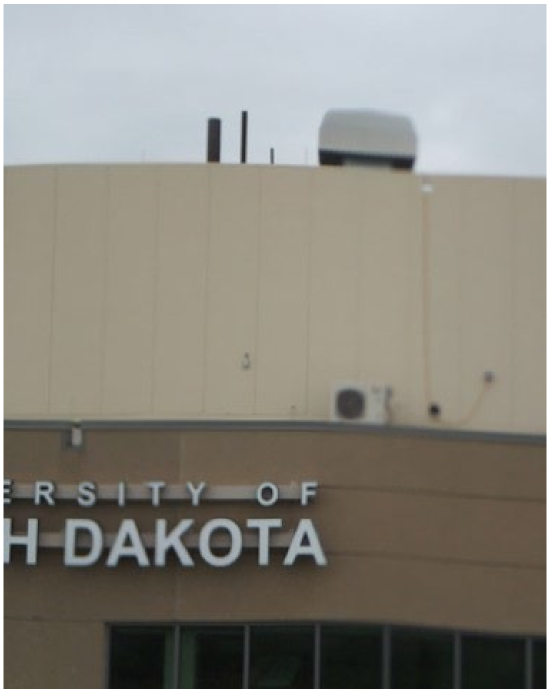


Figure 5-48. Flight 5, image sent on LTE

Figure 5-49. Flight 5, image sent on SATCOM

Table 5-15. Commanded Link Switchover Times for Building Flight 5

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET

Building	5	UA	23-Aug	3:35	LTE	satcom	1257	5000	Y
Building	5	CS	23-Aug	3:35	LTE	satcom	1503	5000	Y
Building	5	UA	23-Aug	3:41	LTE	satcom	1192	5000	Y
Building	5	CS	23-Aug	3:41	LTE	satcom	1053	5000	Y
Building	5	UA	23-Aug	3:43	satcom	LTE	820	5000	Y
Building	5	CS	23-Aug	3:43	satcom	LTE	440	5000	Y

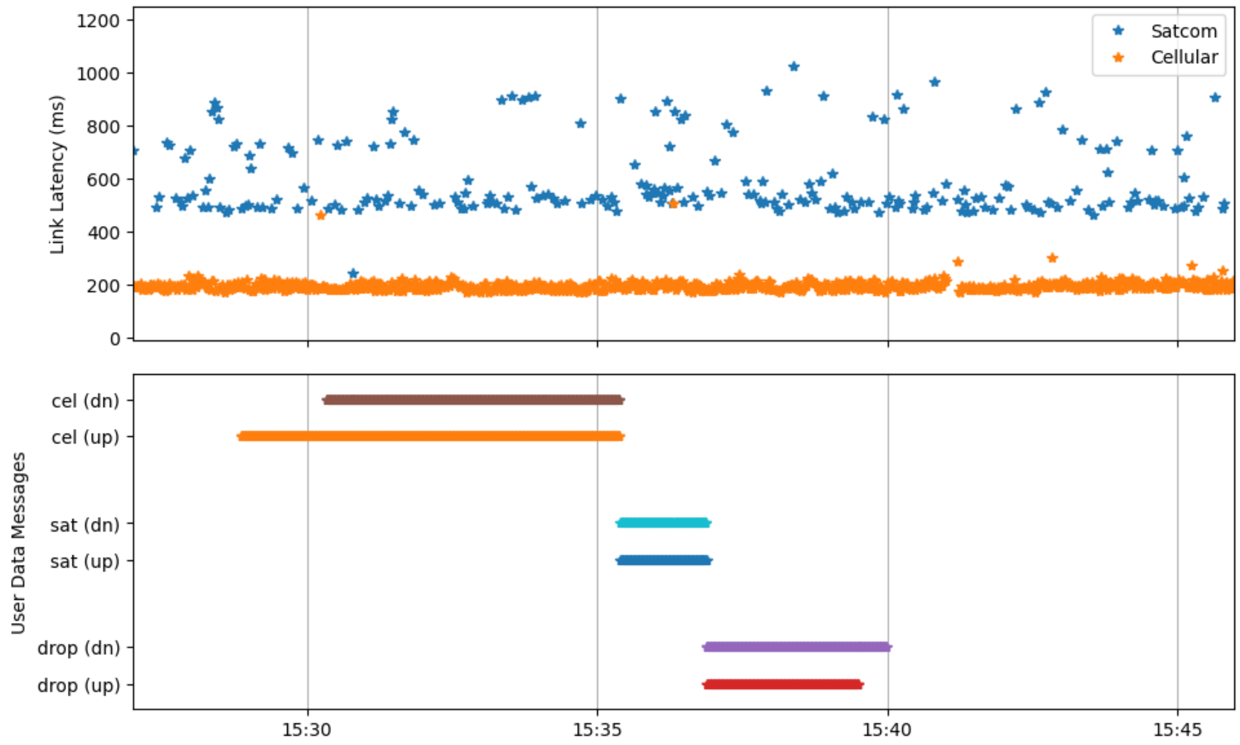


Figure 5-50. Link Latency and User Data Message Stream Path, Building Flight 5

5.1.18 Target C – Building – Flight 6-of-6 (Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under nominal conditions with encryption enabled and link switchovers < TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
B-1	FTS-1 – Target C (Building), Nominal tests, with encryption	6	23 Aug 2023	4:01 CDT	4:14 CDT

General Test Observations: None.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	4:02 CS Status Secure No/No-2 4:02 UA Status Secure No/No-2 4:02 UA Send n=1 4:02/3 CS Status 1/2 Both links up. 4:03 UA status 1/2 Both links up. 4:03 UA Secure Start. Good up secure on LTE. 4:03 CS Status Secure Yes/Yes-2 4:03 UA Status Secure Yes/Yes-2 4:04 CS Starting continuous data stream 4:04 UA starting continuous data stream. seen on wireshark.
TP_CM_004A	User Data exchanges < MTU	PASS	4:05 ARMING / SPINNING / TAKEOFF. 4:05 UA Send n=1 then CS. both good.
TP_CM_004B	User Data exchanges > MTU	PASS	4:07 taking picture day3-flight6-LTE 4:07 downloading picture day3-flight6-LTE
TP_CM_009	Link switchover < TET	PASS	4:08 CS Status 1/2 both links up. Nominal Latencies. 4:08 UA Status 1/2 both links up. 4:08 Switchover switch-1 from lte to satcom. 4:09 UA Status Secure Yes/Yes-1 4:09 CS Status Secure Yes/Yes-1
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	4:09 UA Send n=1 received msg id 6.
TP_CM_004B	User Data exchanges > MTU	PASS	4:09 Taking picture day3-flight6-satcom 4:10 Downloading Picture over satcom
TP_CM_009	Link switchover < TET	PASS	4:11 CS Status 1/2 Both links UP, nominal 4:11 UA Status 1/2 both links up, nominal 4:11 SWITCHOVER Switch-2 from satcom to LTE (Good). 4:11 UA Status Secure Yes/Yes-2 4:11 CS Status secure Yes/Yes-2
TP_CM_007	Control message exchanges	PASS	
TP_CM_004A	User Data exchanges < MTU	PASS	4:12 UA Send n=1 good ID-8 4:12 CS Send n=1 arrived ID-4 (good)
TP_CM_004A	User Data exchanges < MTU	PASS	4:12 LANDED / ON GROUND / Stopped spinning. 4:13 UA Send n=1 ID=10
TP_CM_011	Control / User Plane Termination	PASS	4:13 CS Status Secure Yes/Yes-2 4:13 UA Status Secure Yes/Yes-2 4:13 UA Secure Stop 4:13 CS Status Secure No/No-2 (good). 4:14 UA Status Secure No/No-2 (good) 4:14 UA Send n=1 not received (good)

Detailed Results:

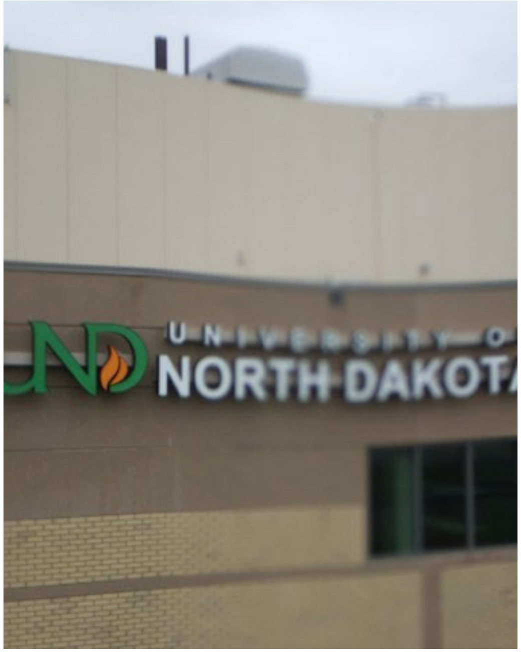


Figure 5-51. Flight 6, picture sent on LTE

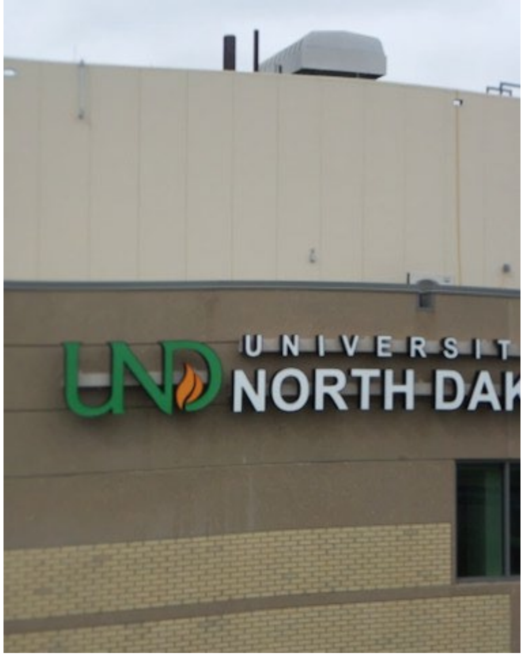


Figure 5-52. Flight 6, picture sent on SATCOM

Table 5-16. Commanded Link Switchover Times for Building Flight 6.

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Building	6	UA	23-Aug	4:08	LTE	satcom	1235	5000	Y
Building	6	CS	23-Aug	4:08	LTE	satcom	1170	5000	Y
Building	6	UA	23-Aug	4:11	satcom	LTE	838	5000	Y
Building	6	CS	23-Aug	4:11	satcom	LTE	415	5000	Y

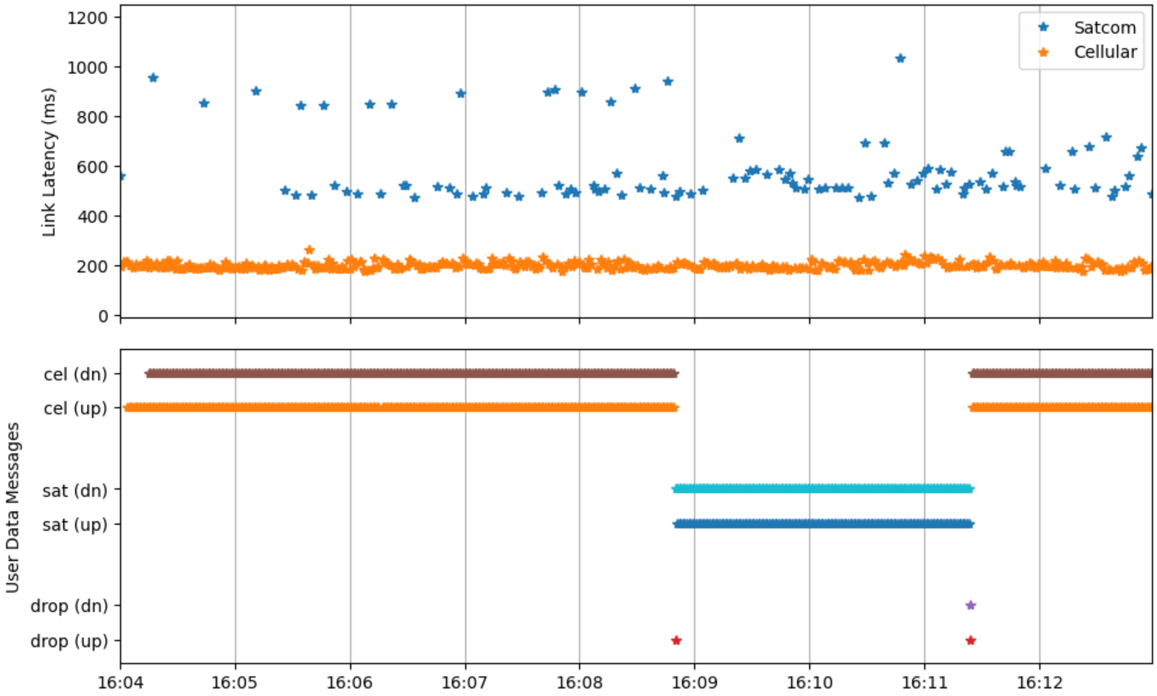


Figure 5-53. Link Latency and User Data Message Stream Path, Building Flight 6

5.1.19 Target C – Building – Flight 1-of-2 (Non-Nominal)

Result = PASS: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under non-nominal conditions with encryption disabled, link interruptions, and link switchovers > TET.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
C-2	FTS-2 – Target C (Building), Non-nominal tests, without encryption	7	23 Aug 2023	4:58 CDT	5:14 CDT

General Test Observations: We performed TP_CM_001 while the aircraft was in the air for this flight. During TP_CM_006, the DTSRs responded to the interruption by switching from LTE to SATCOM.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	4:58 TAKEOFF 4:58 ISSUE/ERROR Carlos noticed anomaly. Forgot Clear_DTSR command. 4:59 Restarted DTSR. 4:59 CS Status Secure No/No-2 4:59 UA Status Secure No/No-2 4:59 n=1 5:00 CS Status 1/2 5:00 UA Status 1/2 Both links up. 5:00 UA Secure Start Good. Secure link over LTE. 5:01 CS Status Secure Both up, Yes/Yes-2 5:01 UA Status Secure Yes/Yes-2 5:01 CS Started continuous sending user data 5:02 UA Starting continuous sending user data.
TP_CM_006	User Data and Control Message Exchange with interruption < TET	PASS	5:05 CS: Disabled link 2, then re-enabled Link-2 Resulted in auto-switchover to Satcom. 5:06 UA Status Secure Yes/Yes-1 5:06 CS Status Secure Yes/Yes-1
TP_CM_005B	User Data exchanges > MTU	PASS	5:06 Taking Picture Day3Flight7-Satcom. good. 5:07 Downloading Picture over Satcom. good. 5:08 UA Status 1/2 Both links UP. nominal from CS, both good.
TP_CM_010	Link switchover > TET with link recovery	PASS	5:09 Disabled both, then Re-enabled both. Disable 2, 1, enable 1, 2. 5:09 Status Secure Yes/Yes-1 on UA, then CS. 5:10 Switchover Switch 2 From Satcom to LTE (good).
TP_CM_008	Control message exchanges	PASS	
TP_CM_005B	User Data exchanges > MTU	PASS	5:10 Taking Picture Day3Flight7-LTE (good) 5:10 Downloading Picture (good)
TP_CM_005A	User Data exchanges < MTU	PASS	5:11 UA Send N=1 received ID=4
TP_CM_005A	User Data exchanges < MTU	PASS	5:11 Cleared for landing. 5:12 Sent N=1, UA, arrived ID=6, CS, ID=2 5:12 approaching for landing.
TP_CM_005A	User Data exchanges < MTU	PASS	5:12 LANDED / ON GROUND / STOPPED 5:13 Send N=1, UA Arrived ID=8.
TP_CM_011	Control / User Plane Termination	PASS	5:13 CS Status Secure Yes/Yes-2 5:13 UA Secure Status Yes/Yes-2 5:14 UA Secure Stop (good). 5:14 CS Status Secure No/No-2, then on UA No/No-2 (good). 5:14 UA Send N=1

Detailed Results:

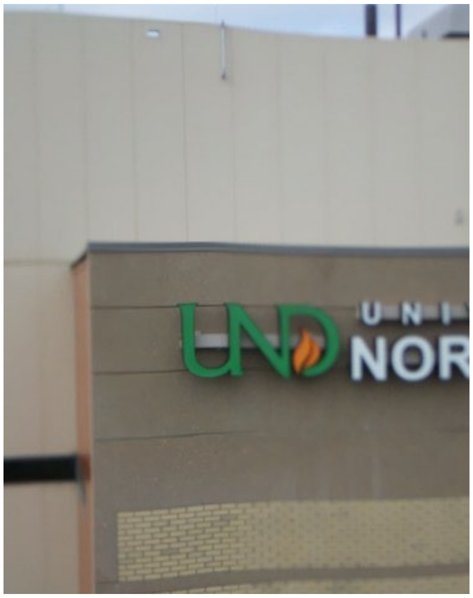


Figure 5-54. Flight 7, picture sent on LTE

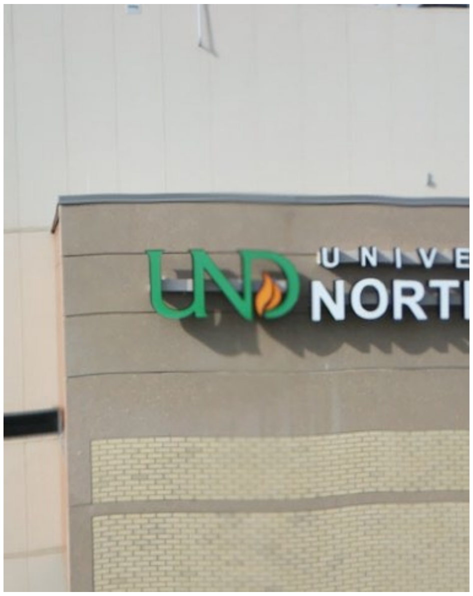


Figure 5-55. Flight 7, pictures sent over SATCOM

Table 5-17. Commanded Link Switchover Times for Building Flight 7

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Building	7	UA	23-Aug	5:10	satcom	LTE	958	5000	Y
Building	7	CS	23-Aug	5:10	satcom	LTE	381	5000	Y

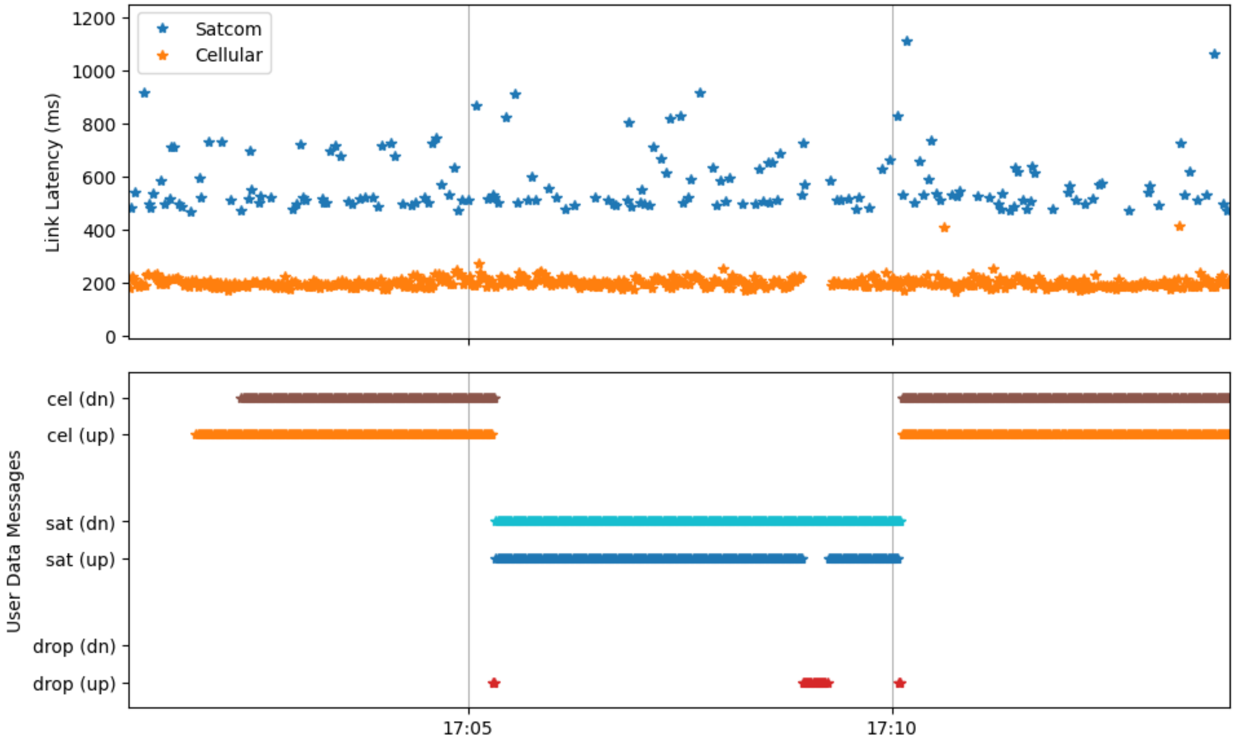


Figure 5-56. Link Latency and User Data Message Stream Path, Non-nominal Flight 1

5.1.20 Target C – Building – Flight 2-of-2 (Non-Nominal)

Result = PARTIAL: This flight test demonstrated Control Plane and User Plane authentication and the exchange of Control Messages and User Data messages (both <MTU and >MTU) under non-nominal conditions with encryption disabled. The procedures to test link interruptions and link switchovers > TET failed.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
C-2	FTS-2 – Target C (Building), Non-nominal tests, without encryption	8	23 Aug 2023	5:26 CDT	5:42 CDT

General Test Observations: The UA and CS DTSRs got out of sync during TP_CM_006. The DTSRs were restarted and this allowed TP_CM_005B to pass, but then the DTSRs did not recover after hitting a software error during TP_CM_010, and all procedures after that failed/were not attempted.

Procedure	Description	Result	Notes
TP_CM_001	Control / User Plane authentication	PASS	5:26 Status Secure both No/No-1 (satcom) 5:26 UA send n=1 5:27 CS Status 1/2 both links up nominal, then on UA (nominal) 5:27 UA Secure START (good, came up on Satcom) 5:27 CS Status Secure Yes/Yes-1 5:28 UA Status Secure Yes/Yes-1 5:28 CS Start sending continuous data stream. 5:29 UA start sending continuous data stream. 5:29 Switchover Switch-1 From Satcom to LTE. (good)
TP_CM_005A	User Data exchanges < MTU	PASS	5:29 Cleared for takeoff. ARMING / SPINNING / TAKEOFF 5:29/30 UA Sending N=1 received ID=4, then CS ID=2
TP_CM_006	User Data and Control Message Exchange with interruption < TET	FAIL	5:30 Disabled LTE and re-enabled (very quick, less that TET) Link came back up on LTE. (Good) 5:31 UA Status Secure Yes/Yes-2. 5:32 CS Status Secure Yes/Yes-1. GUI Shows we're secure on LTE. 5:32 UA Send N=1 (was not received). 5:33 CS. Switch-2 5:33 CS. Status Secure Yes/Yes-2 5:33/34 Send n=1 from UA (twice) was not received. Neither one was received. 5:34 Send N=1 from CS. was not received 5:35 Restarted DTSR's Came up on LTE. (good)
TP_CM_005B	User Data exchanges > MTU	PASS	5:36 Taking Picture Day3-Flight8-LTE. Downloaded (both good).
TP_CM_010	Link switchover > TET with link recovery	FAIL	5:36/37 CS Status 1/2 Both links up, nominal, then from UA,all nominal. 5:37 Disabled Link 1, 2, enabled Link 2, 1. Came back up on LTE. (Disabled for over 5 seconds). 5:38 CS Status Secure Yes/Yes-1 (Satcom), ISSUE/ERROR GUI SHOWS over LTE. 5:39 UA Status Secure Yes/Yes-2 (LTE). The Secure Link did not come up. Secure session was lost. DTSRs went out
TP_CM_005B	User Data exchanges > MTU	NONE	
TP_CM_005A	User Data exchanges < MTU	NONE	
TP_CM_011	Control / User Plane Termination	FAIL	5:41 Cleared to land 5:42 LANDED / ON GROUND / Stopped / Disarmed END OF FLIGHT #8 5:42 Secure Stop on UA. 5:42/3 CS Status Secure : Yes/Yes-1 (ISSUE/ERROR: the secure session was stopped on the UA.) GUI Still shows Secure session on LTE. (Erroneously) ISSUE/ERROR

Detailed Results:

During TP_CM_006, the DTSRs got out of sync when the UA noticed the interruption and switched to LTE from satcom. The CS stayed satcom. At 5:35 the CS Operator restarted the DTSRs in an attempt to recover the system. However in TP_CM_010, the DTSRs got out of sync again, and there was not remaining flight time to resolve the problem.

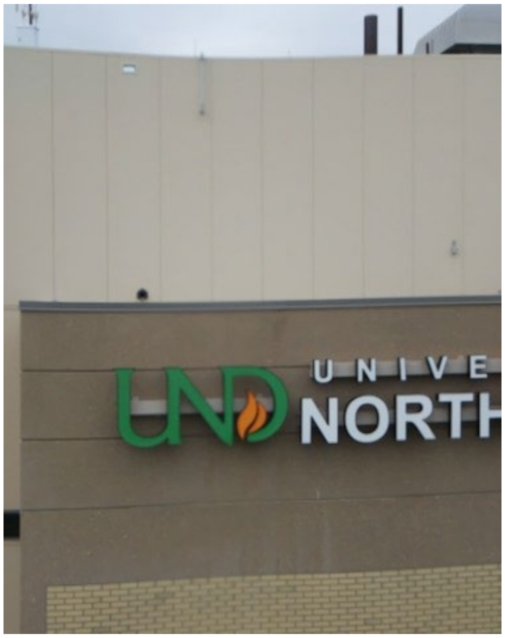


Figure 5-57. Building Flight 8, Picture sent on LTE

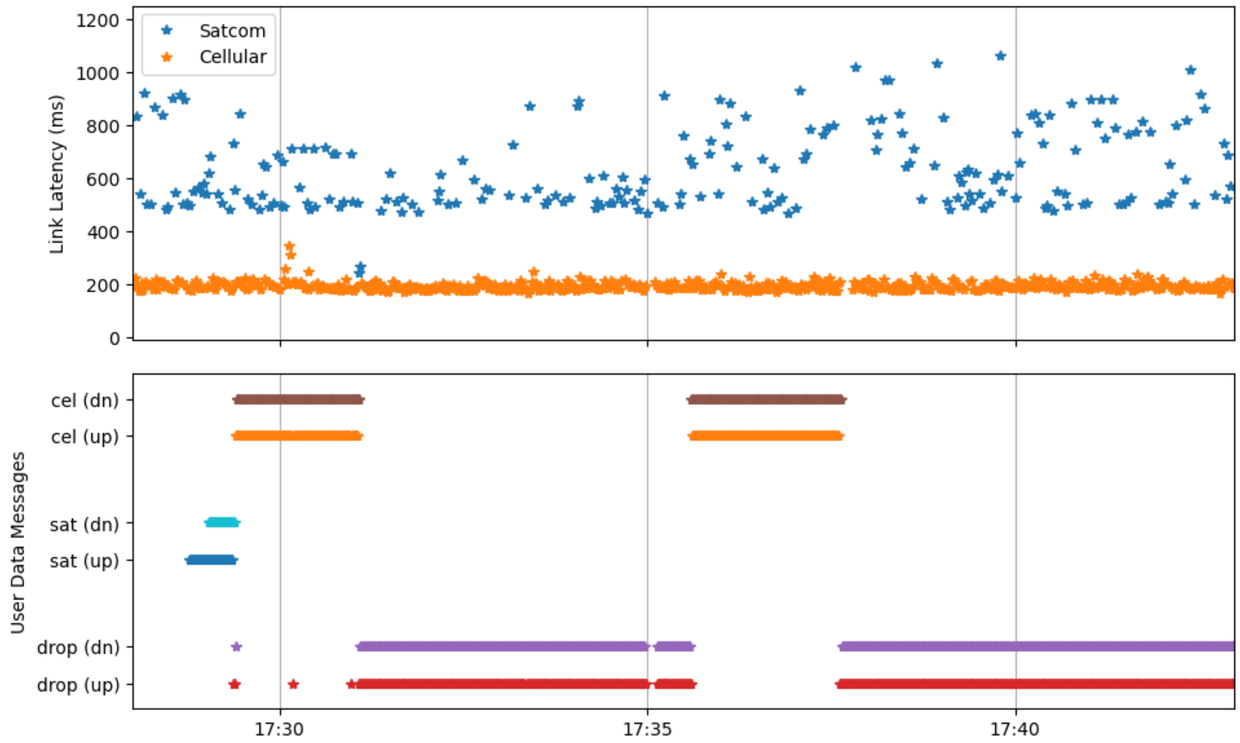


Figure 5-58. Link Latency and User Data Message Stream Path, Non-nominal Flight 2

5.2 GROUND TEST RESULTS

This section documents the results of ground-based test performed in accordance with detailed test procedures specified in [DTP]. Each ground-based test identifies the associated test card (if applicable) and test scenario, the test date, and the test start/end times. General test observations (e.g., issues or unexpected conditions encountered during the ground-based test) are documented. The test results, which are presented in a tabular form, identity the individual test procedures specified, report the result of each test procedure, and provide notes, as necessary, to describe conditions observed during the execution of the specific test procedure and/or to explain a result other than pass.

5.2.1 UA and CS Access Controls

Result = PARTIAL: This ground-based test demonstrated the ability to control access to the UA and to the CS; however, user data messages were transmitted even though a secure user plane connection was not supposed to exist.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
N/A	Ground-based tests of UA/CS access controls	N/A	22 Aug 2023	1:23 CDT	4:07 CDT

General Test Observations: We executed TP_CM_002 three times, and each time, the user data messages are sent by the UA DTSR even though the secure connection was not supposed to exist.

Procedure	Description	Result	Notes
TP_CM_002	Control / User Plane authentication with UA to CS access denied	FAIL	*STARTING TP-CM-002 (3rd Time) 3:47 - CS Status Secure: No/No-2 3:47 - UA Status Secure: No/No-2 3:48 - UA N=1 3:48 - Verifying on UA Main Sniffer... - Verified. 3:49 - Verifying on CS Main Sniffer... – Verified 3:50 - CS LMSF Status 1/2, Satcom Down. LTE=Up. 3:50 - UA LMSF Status 1/2, Satcom down, LTE=up. 3:51 - UA LMSF issuing "Secure Start". 3:51 - Verified on CS Main Sniffer (tun1/tun2) 3:52 - CS. Status Secure: No/No-2 3:52 - UA Status Secure no/no-2 3:52 - UA Send n=1: 3:53 - Verified on CS, and it was actually Received 3:53 - CS send n=1 FAILED, it was actually sent. 3:57 - stopped DTSRs UDMD's LMSF's both sides *FINISHED TP-CM-002 (3rd Time)

All steps passed except step 13 and step 15.

Step 13. The UA DTSR sent the user data even though a secure connection was not supposed to exist.

From the UA DTSR log.

```
2023-08-22 20:52:18.089004 GMT INFO     UdmdIn.cpp:51            Received: ID: 00000010
Origin: UDMD
Cmd: SEND
Size: 63
Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAAA-000010
Sending user data message to peer User Output: Sent 66 bytes.
Buffer Contents: [0542000a00000002  000000040000007f  0000003f00000000  00000000fa466655
2023-08-22 20:52:18.089879 GMT                          00000055442d4141  4141414141414141
4141414141414141  41412d3030303031  3000]
Sent "USER_DATA.REQ          66
```

Step 15. The CS DTSR sent the user data even though a secure connection was not supposed to exist.

From the CS DTSR log.

```
2023-08-22 20:53:45.754253 GMT INFO     UdmdIn.cpp:51            Received: ID: 00000004
Origin: UDMD
Cmd: SEND
Size: 63
Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAAA-000004
Sending user data message to peer User Output: Sent 66 bytes.
Buffer Contents: [0542000400000002  0000000400000000  0000003f00000000  0000000000000000
00000055442d4141  4141414141414141  4141414141414141  41412d3030303030  3400]
Sent "USER_DATA.REQ          66
0400000000000000  3f00000000000000  0000000000000000  55442d4141414141
4141414141414141 414141414141412d  30303030303400]" across secure connection
```

Procedure	Description	Result	Notes
TP_CM_003	Control / User Plane authentication CS to UA access denied	**PASS**	*STARTING procedure TP-CM-003. (times are CDT) 1:23 - CS & UA status secure. CS: No/1 & UA: No/2 1:24 - UA UDMD Send N=1 1:24 - Status 1& 2: both links up on UA first, 1:25 - both links up on CS. Latencies are reasonable. 1:25 - UA LMSF - Secure Start command issued 1:25 - CS LMSF - status secure: No/NO. 1:25 - from CS: Send n=1 1:25 - from UA: Send n=1 1:26 - PASSED Scenario. *End of procedure TP-CM-003.

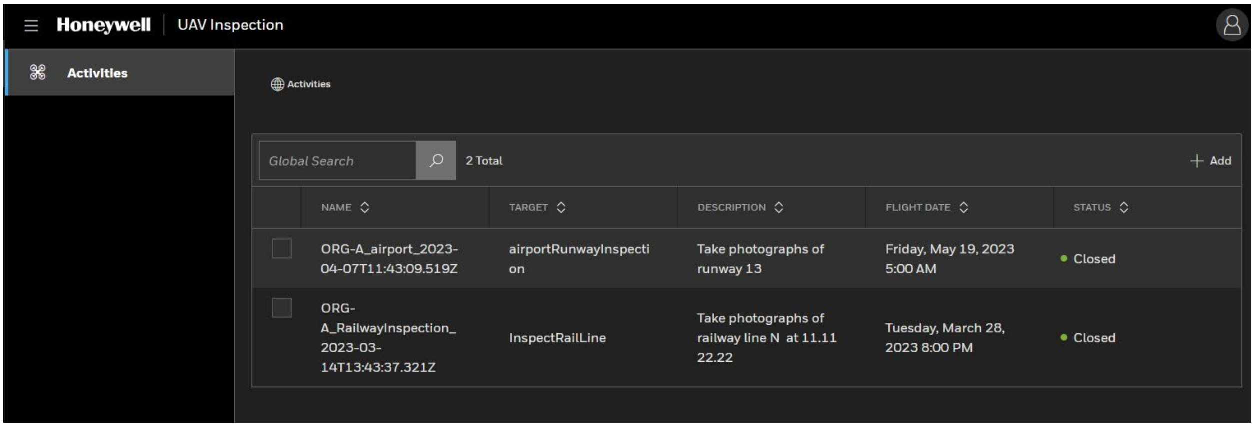
5.2.2 Cloud Storage Access Controls

Result = PASS: This ground-based test demonstrated the ability to control user access to the cloud storage services.

Test Card	Test Scenario Description	Flight#	Date	Start Time	End Time
N/A	Ground-based tests of cloud access controls	N/A	16 Oct 2023	1:30 CDT	1:41 CDT

General Test Observations: None.

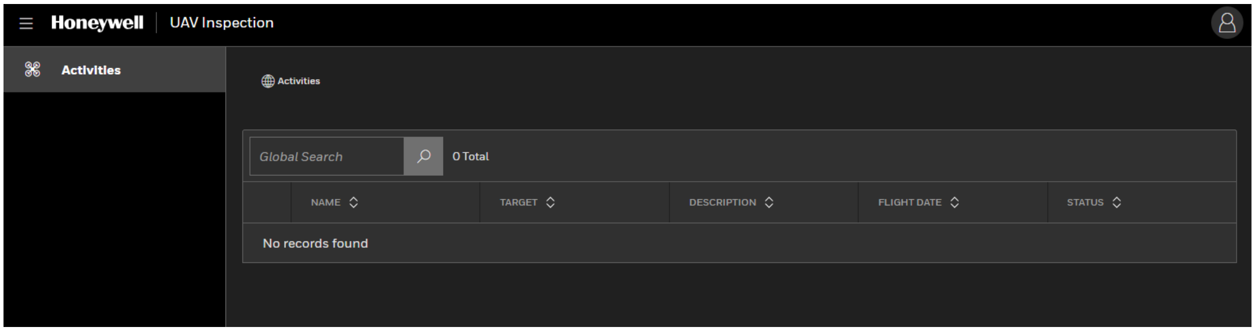
Procedure	Description	Result	Notes
TP_PP_001	Cloud storage access, Valid User with access permitted	**PASS**	When logged in using the credentials of an account with access to user data for organization A, activities for that organization are shown on the dashboard page, as shown in Figure 5-23.
TP_PP_002	Cloud storage access, Valid User with access denied	**PASS**	An account without authorization to access the data of any of the organizations was created on the DSMA. When logged in using valid credentials for that account, the dashboard did not show any of the activities created for the A, B or C organizations, as shown in Figure 5-24.
TP_PP_003	Cloud storage access, Invalid User	**PASS**	Trying to login with an invalid user ID redirects the browser to an invalid user page, as shown in Figure 5-23.



2 Total

	NAME	TARGET	DESCRIPTION	FLIGHT DATE	STATUS
□	ORG-A_airport_2023-04-07T11:43:09.519Z	airportRunwayInspection	Take photographs of runway 13	Friday, May 19, 2023 5:00 AM	● Closed
□	ORG-A_RailwayInspection_2023-03-14T13:43:37.321Z	InspectRailLine	Take photographs of railway line N at 11.11 22.22	Tuesday, March 28, 2023 8:00 PM	● Closed

Figure 5-59: Dashboard for User with Access to Organization A User Data

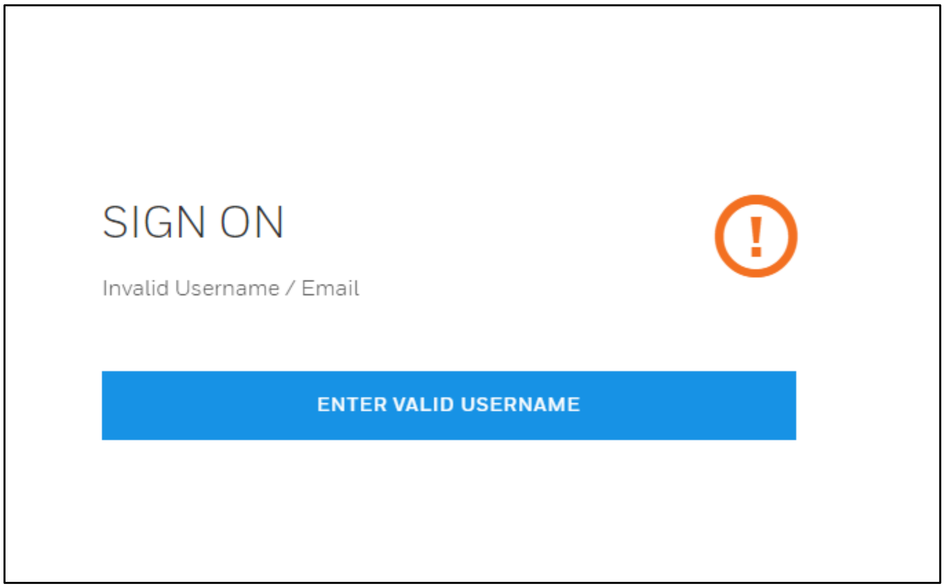


0 Total

	NAME	TARGET	DESCRIPTION	FLIGHT DATE	STATUS

No records found

Figure 5-60: DSMA Dashboard for an Unauthorized User



SIGN ON

Invalid Username / Email

Figure 5-61: Invalid Username Page

5.3 LINK SWITCHOVER TIMING ANALYSIS

During each of the test flights, two link switchover commands were executed while the aircraft was at cruise. In summary, a total of 68 link switchover commands were executed. Each switchover was measured at both the UA and the CS systems, even though the command always initiated from the UA. Consequently, the switchover time at the UA was always slightly longer than at the CS. Out of the 68 switchovers, no switchover exceeded the TET. The switchover times are recorded in Table 23. On average, a link switchover from LTE to SATCOM took 715 ms, while SATCOM to LTE switchovers took about twice that long, 1406 ms on average.

Table 18. Switchover Times for all commanded Link Switchovers

Target	Flight No	System	Date	Time (CDT)	From	To	Switchover time (ms)	TET	<TET
Water Tower	1	UA	24-Aug	12:11	satcom	LTE	1038	5000	Y
Water Tower	1	CS	24-Aug	12:11	satcom	LTE	408	5000	Y
Water Tower	1	UA	24-Aug	12:13	LTE	satcom	1223	5000	Y
Water Tower	1	CS	24-Aug	12:14	LTE	satcom	1701	5000	Y
Water Tower	2	UA	24-Aug	1:07	LTE	satcom	1258	5000	Y
Water Tower	2	CS	24-Aug	1:07	LTE	satcom	1817	5000	Y
Water Tower	2	UA	24-Aug	1:10	satcom	LTE	797	5000	Y
Water Tower	2	CS	24-Aug	1:10	satcom	LTE	362	5000	Y
Water Tower	3	UA	24-Aug	1:31	LTE	satcom	1135	5000	Y
Water Tower	3	CS	24-Aug	1:31	LTE	satcom	1331	5000	Y
Water Tower	3	UA	24-Aug	1:34	satcom	LTE	824	5000	Y
Water Tower	3	CS	24-Aug	1:34	satcom	LTE	367	5000	Y
Water Tower	4	UA	24-Aug	1:58	LTE	satcom	1146	5000	Y
Water Tower	4	CS	24-Aug	1:58	LTE	satcom	1853	5000	Y
Water Tower	4	UA	24-Aug	2:00	satcom	LTE	851	5000	Y
Water Tower	4	CS	24-Aug	2:00	satcom	LTE	412	5000	Y
Water Tower	5	UA	24-Aug	2:20	LTE	satcom	1995	5000	Y
Water Tower	5	CS	24-Aug	2:20	LTE	satcom	1606	5000	Y
Water Tower	5	UA	24-Aug	2:24	satcom	LTE	1844	5000	Y
Water Tower	5	CS	24-Aug	2:24	satcom	LTE	391	5000	Y
Water Tower	6	UA	24-Aug	2:56	LTE	satcom	1921	5000	Y
Water Tower	6	CS	24-Aug	2:56	LTE	satcom	1428	5000	Y
Water Tower	6	UA	24-Aug	2:59	satcom	LTE	1062	5000	Y
Water Tower	6	CS	24-Aug	2:59	satcom	LTE	351	5000	Y
Walking Path	1	UA	24-Aug	3:51	LTE	satcom	1120	5000	Y
Walking Path	1	CS	24-Aug	3:51	LTE	satcom	1030	5000	Y
Walking Path	1	UA	24-Aug	3:54	satcom	LTE	858	5000	Y
Walking Path	1	CS	24-Aug	3:54	satcom	LTE	399	5000	Y
Walking Path	2	UA	24-Aug	4:15	satcom	LTE	798	5000	Y
Walking Path	2	CS	24-Aug	4:15	satcom	LTE	484	5000	Y
Walking Path	2	UA	24-Aug	4:19	satcom	LTE	795	5000	Y
Walking Path	2	CS	24-Aug	4:19	satcom	LTE	345	5000	Y
Walking Path	3	UA	24-Aug	4:49	satcom	LTE	465	5000	Y
Walking Path	3	CS	24-Aug	4:49	satcom	LTE	950	5000	Y
Walking Path	3	UA	24-Aug	4:50	LTE	satcom	1862	5000	Y
Walking Path	3	CS	24-Aug	4:50	LTE	satcom	1888	5000	Y

Walking Path	4	UA	24-Aug	5:18	LTE	satcom	1189	5000	Y
Walking Path	4	CS	24-Aug	5:18	LTE	satcom	1637	5000	Y
Walking Path	4	UA	24-Aug	5:30	satcom	LTE	1039	5000	Y
Walking Path	4	CS	24-Aug	5:30	satcom	LTE	368	5000	Y
Walking Path	5	UA	24-Aug	6:00	LTE	satcom	1258	5000	Y
Walking Path	5	CS	24-Aug	6:00	LTE	satcom	1475	5000	Y
Walking Path	5	UA	24-Aug	6:02	LTE	satcom	1514	5000	Y
Walking Path	5	CS	24-Aug	6:02	LTE	satcom	427	5000	Y
Walking Path	6	UA	24-Aug	6:20	LTE	satcom	1153	5000	Y
Walking Path	6	CS	24-Aug	6:20	LTE	satcom	2043	5000	Y
Walking Path	6	UA	24-Aug	6:30	satcom	LTE	1272	5000	Y
Walking Path	6	CS	24-Aug	6:30	satcom	LTE	418	5000	Y
Building	1	UA	23-Aug	1:19	LTE	satcom	1706	5000	Y
Building	1	CS	23-Aug	1:19	LTE	satcom	1276	5000	Y
Building	1	UA	23-Aug	1:23	satcom	LTE	1141	5000	Y
Building	1	CS	23-Aug	1:23	satcom	LTE	400	5000	Y
Building	4	UA	23-Aug	3:09	LTE	satcom	1193	5000	Y
Building	4	CS	23-Aug	3:09	LTE	satcom	1214	5000	Y
Building	4	UA	23-Aug	3:12	satcom	LTE	1540	5000	Y
Building	4	CS	23-Aug	3:12	satcom	LTE	393	5000	Y
Building	5	UA	23-Aug	3:35	LTE	satcom	1257	5000	Y
Building	5	CS	23-Aug	3:35	LTE	satcom	1503	5000	Y
Building	5	UA	23-Aug	3:41	LTE	satcom	1192	5000	Y
Building	5	CS	23-Aug	3:41	LTE	satcom	1053	5000	Y
Building	5	UA	23-Aug	3:43	satcom	LTE	820	5000	Y
Building	5	CS	23-Aug	3:43	satcom	LTE	440	5000	Y
Building	6	UA	23-Aug	4:08	LTE	satcom	1235	5000	Y
Building	6	CS	23-Aug	4:08	LTE	satcom	1170	5000	Y
Building	6	UA	23-Aug	4:11	satcom	LTE	838	5000	Y
Building	6	CS	23-Aug	4:11	satcom	LTE	415	5000	Y
Building	7	UA	23-Aug	5:10	satcom	LTE	958	5000	Y
Building	7	CS	23-Aug	5:10	satcom	LTE	381	5000	Y

6 SUMMARY AND RECOMMENDATIONS

This section provides an overall assessment of the test/inspection results, and where appropriate, provides lessons learned and recommendations for further testing.

6.1 SUMMARY

The objective of the UAS-PP project was to demonstrate a scalable security solution that uses industry-proven cybersecurity technology for the protection of information (in this case, images) that are transferred from a UAS to a ground control station and then made available to ground users via a commercial cloud storage service. The Key Performance Indicators (KPIs) and metrics for the UAS Privacy Protections Project are captured in Table 24, where the final column indicates that all metrics were met at the conclusion of this project.

Table 19. KPIs and metrics for Privacy Protections

No.	KPI	Metric	Met/ Not Met
1.0	Level of Preparedness	C2 systems patched, vulnerability scans	Met
2.1	Compliance with RTCA DO-377A C2 Link System MASPS Security Requirements	Protect user plane traffic between the UA and the CS	Met
2.2		Protect control plane traffic between the UA and the CS	Met
2.3		Protect user plane traffic between the UA and the air/ground network gateway	Met
2.4		Protect control plane traffic between the UA and the air/ground network gateway	Met
2.5		Protect user plane traffic between the air/ground network gateway and the CS	Met
2.6		Protect control plane traffic between the air/ground network gateway and the CS	Met
3.1	Access Management	Individual operators are able to access only their operator-specific data stored in operator-partitioned cloud storage	Met
3.2		Number of users with administrative privileges (i.e., enforce principle of least privilege)	Met

As described in the [STP] and [DTP], the team planned 11 inspections, two ground tests, 20 test flights, and System Security Verification (SSV) testing on the UAS-PP system. All inspections and tests were successfully performed. The tests and inspections largely passed, and in the cases of failures, this report outlines why the failure occurred. The team advanced the TRL for the C2 system and the Honeywell VersaWave SATCOM system, improved the GFE software, and identified ways to advance the GFE software in future productization efforts. Improvements and weaknesses within the security framework in the UAS-PP are identified, should a future team seek to expand on this work. The UAS-PP tests and inspections successfully demonstrated that the security requirements from DO-377A can be implemented on a C2 system and applied to protect a user data stored on a commercial cloud service.

6.2 RECOMMENDATIONS AND LESSONS LEARNED

6.2.1 Program Management Lessons Learned

Contractual delays between Honeywell and NPUASTS prevented the companies from procuring hardware on time as per the planned schedule. The delayed hardware procurement prevented hardware integration with the C2 software. Ideally, hardware and software integration would have been completed months prior to the flight demonstration as integration reduces technical risk. Our resulting schedule was so compressed that several integration issues were not resolved before our flight testing, and troubleshooting these issues consumed much of our time onsite at NPUASTS. Future programs facing contractual delays might consider purchasing equipment at risk to mitigate the technical risk of delaying integration.

6.2.2 Recommendations and Lessons Learned for Future Flight Tests

6.2.2.1 INTEGRATION TESTING

We recommend that future teams budget time for the software team to be collocated with the hardware to perform integration testing. Remote software developers faced challenges with VPNs and network access that were overcome by being physically located in the lab. Future programs should plan for developers to be onsite for the duration of the integration and test phase.

Future programs should plan several days where the team has access to the aircraft for hardware integration, mounting, and ground based validation of the system on the aircraft before engaging the flight crews. Mounting of antennas is not trivial and affects the RF performance considerably. Future programs should engage with RF engineers to verify the planned antenna mounting to the aircraft. It was helpful for us to share pictures of our planned mounting solution with antenna experts to get their feedback. Teams should avoid making assumptions about how antennas work and instead directly engage with the designer or supplier to get a mutual understanding of ideal mounting locations and system operation; these conversations can occur early in a program. Once the antenna mounting solution is identified, teams should plan flight tests specifically to verify the mounting of each system.

Troubleshooting interference issues requires data collection with each component transmitting, one by one. A methodical approach is required; therefore, interference testing cannot be rushed and should be undertaken only when the final configuration is ready.

6.2.3 Software Improvements to the C2 Application

Existing switchover controls in the GFE software showed some limitations during the UAS-PP project that were corrected before the flights commenced for the UAS-C2 project. These software limitations arose from a couple of factors. Firstly, the UA and CS DTSRs could be out of sync with regard to the availability of any link for some brief time. Having a different assessment of the link availability sometimes made each DTSR choose different links as the most appropriate link to try attempt for a switchover. Secondly, once the DTSRs decided what link to try, the DTSR did not try any other link if it could not connect over it. Consequently, the UA and CS DTSRs were prone to getting stuck in a live-lock situation, hopelessly trying to connect with each other over different links. To avoid this problem, the C2 application software was changed after the UAS-PP flights, but before the UAS-C2 flights so that each DTSR would try to connect with the remote peer over every link, following a process that ensures convergence on a link that is available to both. This process continues uninterrupted until the DTSRs complete the switchover handshake over one of the links. To avoid discarding any switchover candidate links due to transient link status, both DTSRs try all links, regardless of availability status. Although this process might waste some time trying links that might be down in some situations, it ensures the UA and CS DTSRs will have the opportunity to test every link in a finite amount of time.

DTLS session establishment control software was also updated for the C2 test flights. Existing software required the CS DTSR to be running before its peer was brought up. The UA announced its availability to the CS with a single clear text message at start up. If the CS DTSR missed that message, it would reject the request to connect. This required the preferred link and the CS DTSR to be up on both sides before the UA DTSR could be started. In the new software, the UA announces its availability with some frequency, for as long as necessary, whenever a DTLS session is not active. This change allows the UA to make itself ready to initiate the DTLS handshake at any time.

6.2.4 Software Development Considerations

A significant source of issues during integration and testing came from components used to condition traffic for each of the IPv4 links. The associated risks can be mitigated in future implementations by requiring the following from each link solution:

1. Integrated VPN tunnel or similar traffic encryption support for defense in depth. Requiring the CS or UA to implement traffic encryption support impacts scalability and increases complexity.
2. Integrated framing protocol to facilitate tolerance of partial packet drops.
3. Integrated throttle control for UDP traffic over low data rate links.
4. Better, more regular access to control functions (e.g. device reset, config, status)

The high-level architecture of the software lends itself nicely to supporting C2 operations. Major modules correspond to well-defined aspects of the functionality involved. Interactions are well-defined and appropriate. However, some of the lower-level design choices have proven to be problematic. The following issues should be addressed in a production version of the C2 software:

1. A thread manager pattern is used extensively throughout the code for many of the components. Although it is well defined and useful for quick development, it results in the proliferation of Inter-Process Communication (IPC) queues and read/write threads and promotes unnecessary message exchanges between threads within the same processes.
   - This might have a negative impact on performance since additional message copies need to be made and additional context switches are required for queue processing.
   - Decreases maintainability since it is more difficult to follow the messages through all queues and threads.
   - The use of multiple threads and IPCs could be replaced by a limited number of threads.
2. Many error conditions are not handled gracefully. Many components/threads will abort execution after hitting an error condition.
3. Triggering of session establishment is not implemented from the CS LMSF.
4. Many components have duplicate code.
5. No continuous integration support nor automated end-to-end tests.
6. No regular mechanism for user apps to interact with core C2 software beyond sending user data. LMSF test driver should be replaced by APIs that allow user applications to send commands to and handle notifications from the core C2 link management software.

Finally, manual adjustment of the DTLS_TIMEOUT_INIT parameter in the WolfSSL library file ./wolfssl/wolfssl/internal.h might be necessary to allow the software to complete the DTLS session establishment handshake over high-latency links. A value of four seconds worked well for the Satcom link for both projects.

6.2.5 C2 Link Routing Approach

Our implementation of the DTSRs use *C2 Link System Route Switchovers* (optional procedure 2, as presented in [DO-377A] (section 5.2.2)). In this type of procedure, the DTSRs rely on a single mapping from IPv6-to-IPv4 addresses in each direction to select the network link to use for user data and control message exchanges. When compared with the connection approach (optional procedure 1), route switchovers offer the advantage of having a single IPv6 address for each side of the C2 link throughout the whole network. However, it depends on maintaining the consistency of the two mappings across the network in a timely manner. This can be thought of, in general, as maintaining a consistent distributed state. For example, the second and third flights at the Building for 005 PP illustrated a software problem that can occur when one DTSR gets out of sync with the peer; in our case, the UA and CS DTSRs were talking on different tunnels and unable to communicate after hitting this condition. We assert that any implementation of this procedure would need to support scenarios where these mappings are, at least temporarily and possibly permanently, inconsistent throughout the network. Maintaining consistency reliably in the presence of faults is a difficult problem. Therefore, such provisions will ultimately add significant complexity to the software to safely support UAVs in real operational environments.

An approach consistent with *Multilink Operations*, as presented in [DO-377A] (section K.5.2.3), might be used to implement what can be referred to as continuous switchovers or stateless redundancy. This alternate approach would eliminate the need to declare and maintain a single IPv4 link as the *active* link. Instead, each DTSRs would be able to send and receive messages over any of the available links, eliminating the need to maintain a consistent distributed state across the network at all times. Link preference can be decided for each individual data message, if desired. Alternatively, virtual user plane channels can be defined; for example, each user plane channel can have various throughput and latency requirements such that the DTSRs can make different routing decisions based on what channel is selected for each message by a user application.

Make-before-Break (MbB) switchovers require user data traffic to be sent over the active IPv4 link, while control messages are sent over the new link to setup the switchover. Since traditional IP routing can only provide one route per destination IP address at a given time, this kind of routing cannot be used to support the MbB behavior. The DTSRs in our implementation use traditional IP routing and therefore must stop sending user data before control messages can be sent over the new link. An alternative implementation might use policy-based routing to incorporate the destination ports for the user and control plane traffic to the routing criteria, enabling the routing of control and user traffic over different IPv4 links at the same time. Leveraging TunTap interfaces and the IP stack multiplexing functions to implement the UDMD proved to be an efficient and productive choice. This affords the following benefits:

- Collaborating user applications running on the UA and CS could communicate with each other using the well-known socket API without regard to lower level C2 link management behavior.

- User App development is largely decoupled from the availability of a C2 link subsystem. Most of it can proceed in easily accessible simulated network environments.
- Leverages maturity, availability, reliability, updatability and efficiency of existing IP stack implementations.

For next steps, Honeywell has considered how to progress the UAS work accomplished under this project, and made submissions under Call 004 and Call 005 BAA that outline our recommended path forward in this area. In these whitepapers, Honeywell plans to incorporate the lessons learned from this project and flight test these improvements and additional features that Honeywell has matured to at least TRL 5.

A. EXPECTED RESULTS

This appendix documents the expected results for the verification steps in each test procedure. The results of post-flight analyses are compared with the expected results to ascertain compliance or identify deviations.

A.1 COMMON TEST PROCEDURES

A.1.1 TP_CM_001 – Control Plane and User Plane Traffic Mutual Authentication with User Plane Traffic Access Control Allowed

STEP	REQ	Action	Component	Description	Procedure

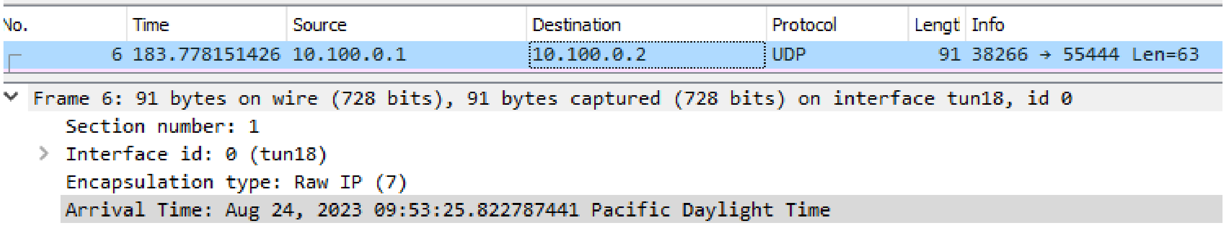
1	IR-03	VERIFY	CS LMSF console	CS status shows <u>no</u> secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: `**N**`/<ID> |`
					`Control: `**N**`/<ID>`

```
2023-08-24 16:52:58.364512 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

2	IR-03	VERIFY	UA LMSF console	UA status shows <u>no</u> secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: `**N**`/<ID> |`
					`Control: `**N**`/<ID>`

```
2023-08-24 16:53:10.072297 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

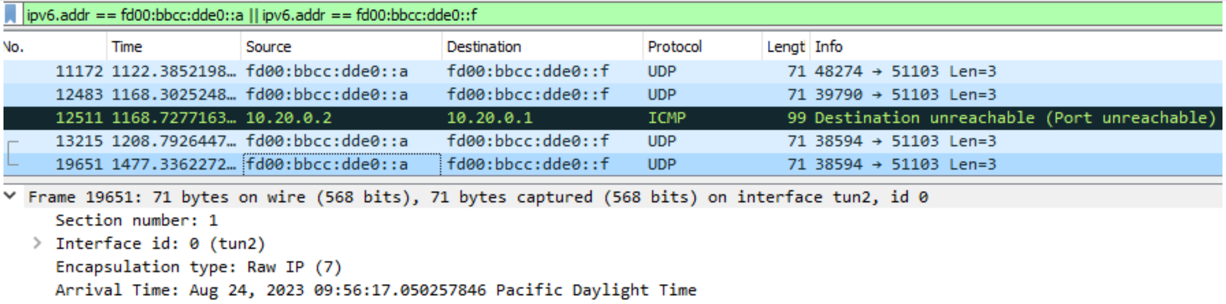
3	IR-03	SEND	UA User Sniffer	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 09:53 PDT (11:53 CDT)



```
No.   Time            Source       Destination   Protocol   Lengt Info
    6 183.778151426   10.100.0.1   10.100.0.2    UDP           91 38266 → 55444 Len=63

Frame 6: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
    Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 09:53:25.822787441 Pacific Daylight Time
```

4	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	Verify via the traffic sniffer log that the User Data message was not sent by the UA DTSR at 9:53 PDT (16:53 GMT)

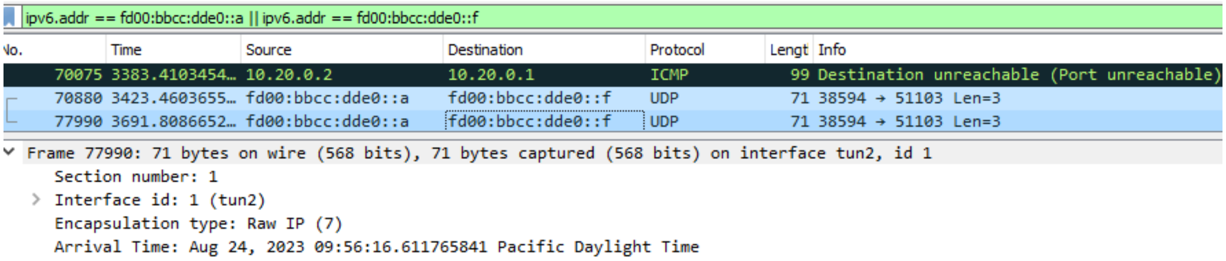
STEP	REQ	Action	Component	Description	Procedure



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f
No.     Time              Source              Destination         Protocol  Lengt Info
  11172 1122.3852198… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 48274 → 51103 Len=3
  12483 1168.3025248… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 39790 → 51103 Len=3
  12511 1168.7277163… 10.20.0.2           10.20.0.1           ICMP         99 Destination unreachable (Port unreachable)
  13215 1208.7926447… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 38594 → 51103 Len=3
  19651 1477.3362272… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 38594 → 51103 Len=3
Frame 19651: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 09:56:17.050257846 Pacific Daylight Time
```

Or the UA DTSR:
2023-08-24 16:53:25.822974 GMT INFO UdmdIn.cpp:51
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 09:53 PDT



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f
No.     Time              Source              Destination         Protocol  Lengt Info
  70075 3383.4103454… 10.20.0.2           10.20.0.1           ICMP         99 Destination unreachable (Port unreachable)
  70880 3423.4603655… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 38594 → 51103 Len=3
  77990 3691.8086652… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   UDP          71 38594 → 51103 Len=3
Frame 77990: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 09:56:16.611765841 Pacific Daylight Time
```

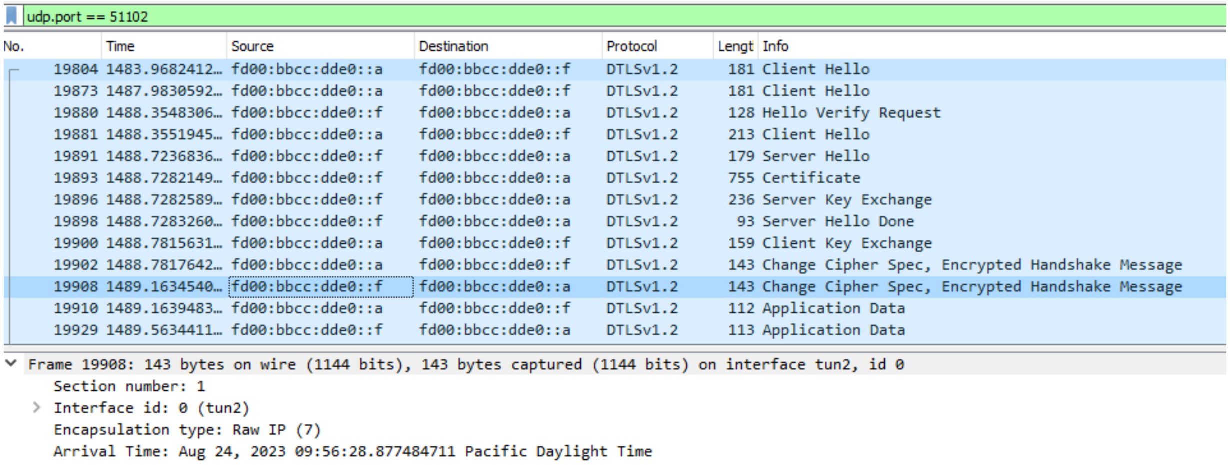
6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					`Expected output`
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	`cs-sh lmsf`
					`lmsf> Status 1`
					`Status 2`
					`Status 3`
					
					Expected output
					`Link 1 Up`
					`Link 2 Up`
					`Link 3 Up`

8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	`cs-sh lmsf`
					`lmsf> secure start`

```
From UA DTSR Log:
2023-08-24 16:56:18.050748 GMT INFO     ControlOut.cpp:193
Enabling secure session
```

STEP	REQ	Action	Component	Description	Procedure
9	IR-01 SER-08	OBSERVE	CS Main Sniffer	Secure session establishment are exchanged over the selected link	Observe secure session establishment messages exchanged



```
udp.port == 51102

No.    Time           Source              Destination         Protocol   Lengt Info
 19804 1483.9682412… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello
 19873 1487.9830592… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello
 19880 1488.3548306… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    128 Hello Verify Request
 19881 1488.3551945… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    213 Client Hello
 19891 1488.7236836… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    179 Server Hello
 19893 1488.7282149… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    755 Certificate
 19896 1488.7282589… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    236 Server Key Exchange
 19898 1488.7283260… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2     93 Server Hello Done
 19900 1488.7815631… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    159 Client Key Exchange
 19902 1488.7817642… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    143 Change Cipher Spec, Encrypted Handshake Message
 19908 1489.1634540… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    143 Change Cipher Spec, Encrypted Handshake Message
 19910 1489.1639483… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    112 Application Data
 19929 1489.5634411… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    113 Application Data

Frame 19908: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 09:56:28.877484711 Pacific Daylight Time
```

10	IR-07
	SER-07
	SER-08
		VERIFY	CS LMSF console	CS status shows:
				…secure session is established
				…which link is providing the connection
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

```
CS DTSR
2023-08-24 16:56:36.505869 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

11	IR-07
	SER-07
	SER-08
		VERIFY	UA LMSF console	UA status shows:
				…secure session is established
				…which link is providing the connection
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/3 | Control: Y/3`

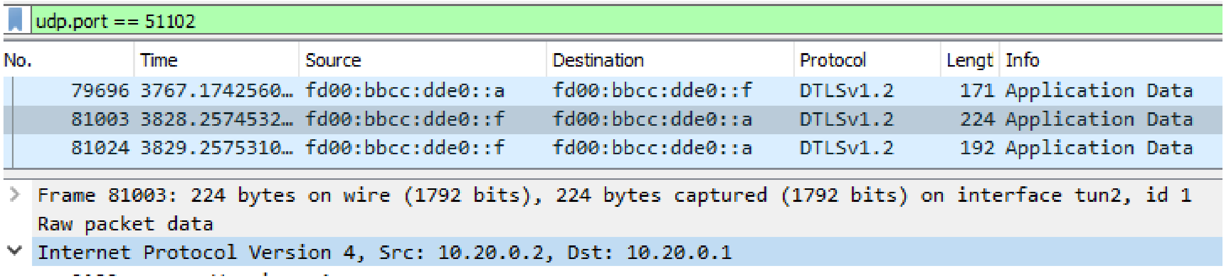
```
UA DTSR
2023-08-24 16:56:46.874857 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

12	IR-03	SEND	CS OS Console	Send User Data from CS to UA at a rate less than TET and size less than MTU	`uas-msg-sim cs`
13	IR-03	SEND	UA OS Console	Send User Data from UA to CS at a rate less than TET and size less than MTU	`uas-msg-sim ua`

Post-test Log Analysis

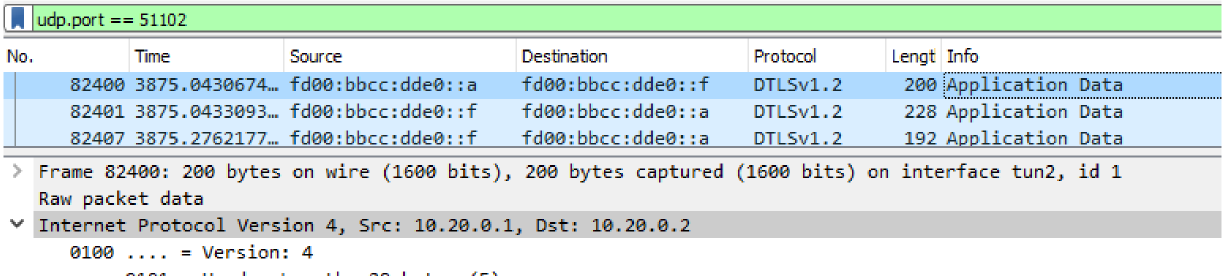
STEP	REQ	Action	Component	Description	Procedure
14	IR-03 IR-04 IR-02	VERIFY	CS Main Sniffer	User Data is sent and received by the CS DTSR on the active link	Verify via the traffic sniffer log that: a) User Data messages were sent by the CS DTSR b) User Data messages were sent only via the link supporting the active connection c) User Data messages were received by the CS DTSR d) User Data messages were received only via the link supporting the active connection e) User Data and Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

a and b) Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE



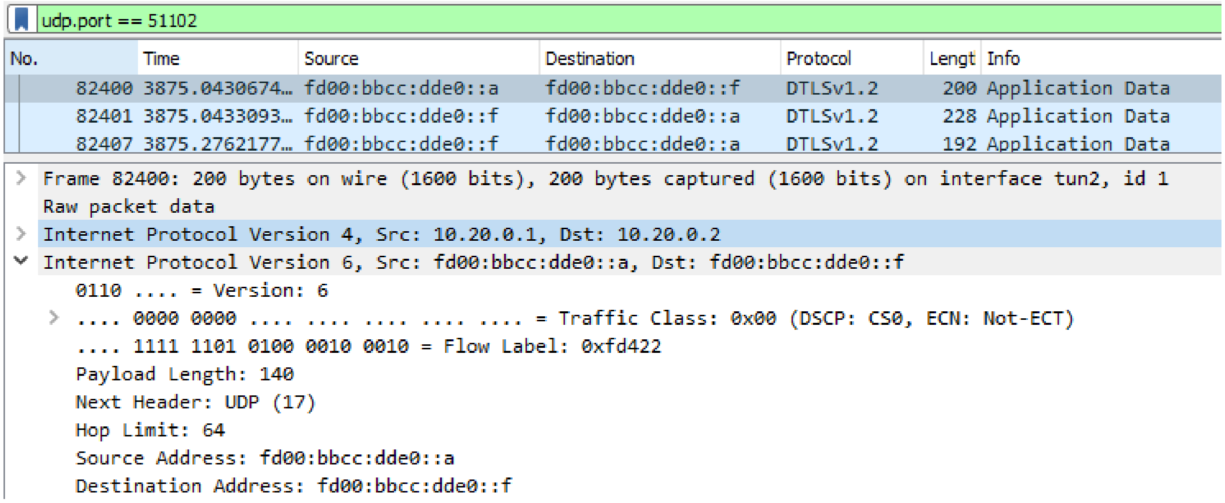
```
udp.port == 51102

No.    Time             Source              Destination         Protocol   Lengt Info
 79696 3767.1742560…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    171 Application Data
 81003 3828.2574532…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    224 Application Data
 81024 3829.2575310…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    192 Application Data

> Frame 81003: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
```

C and d) Source address 10.20.0.1 is UA on LTE; destination address of 10.20.0.2 is CS on LTE



```
udp.port == 51102

No.    Time             Source              Destination         Protocol   Lengt Info
 82400 3875.0430674…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    200 Application Data
 82401 3875.0433093…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    228 Application Data
 82407 3875.2762177…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    192 Application Data

> Frame 82400: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
     0100 .... = Version: 4
```

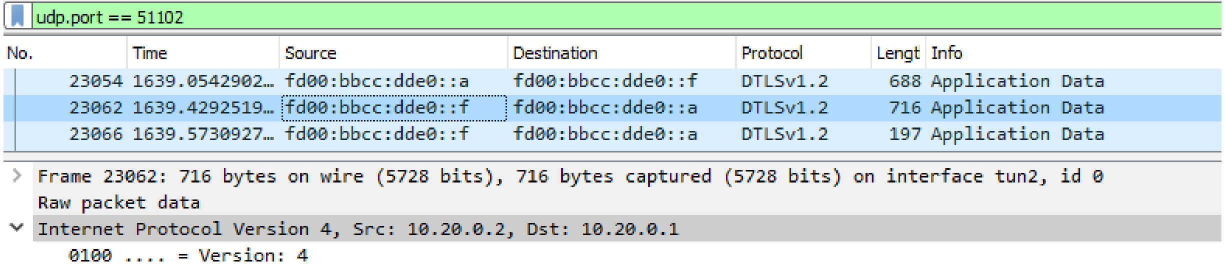
e) IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR



```
udp.port == 51102

No.    Time             Source              Destination         Protocol   Lengt Info
 82400 3875.0430674…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    200 Application Data
 82401 3875.0433093…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    228 Application Data
 82407 3875.2762177…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    192 Application Data

> Frame 82400: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface tun2, id 1
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
     0110 .... = Version: 6
   > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
     .... 1111 1101 0100 0010 0010 = Flow Label: 0xfd422
     Payload Length: 140
     Next Header: UDP (17)
     Hop Limit: 64
     Source Address: fd00:bbcc:dde0::a
     Destination Address: fd00:bbcc:dde0::f
```

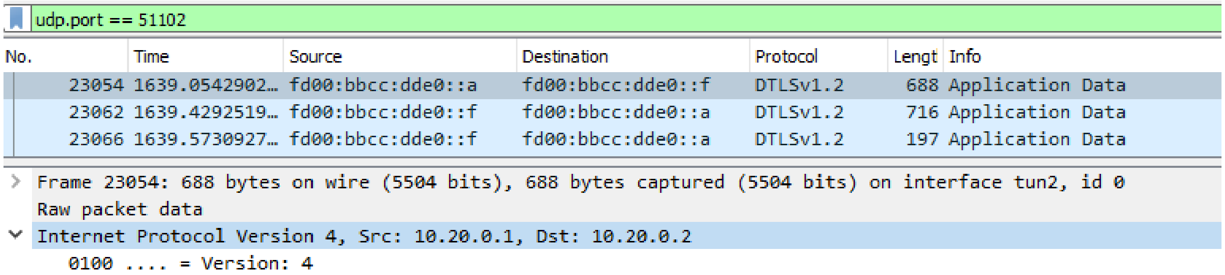
STEP	REQ	Action	Component	Description	Procedure
15	IR-03 IR-04 IR-02	VERIFY	UA Main Sniffer	User Data is sent and received by the UA DTSR on the active link	Verify the via traffic sniffer log that: a) User Data messages were received by the UA DTSR b) User Data messages were received only via the link supporting the active connection c) User Data messages were sent by the UA DTSR d) User Data messages were sent only via the link supporting the active connection e) User Data and Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

A and B) Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE



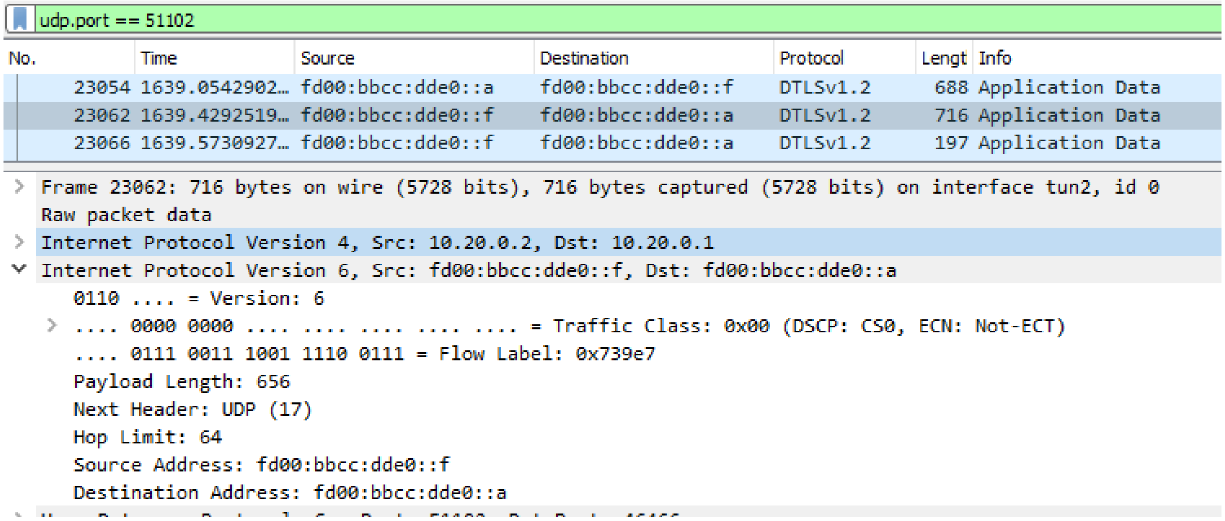
```
udp.port == 51102

No.    Time                Source              Destination         Protocol   Lengt Info
23054  1639.0542902…       fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   688   Application Data
23062  1639.4292519…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   716   Application Data
23066  1639.5730927…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   197   Application Data

> Frame 23062: 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface tun2, id 0
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
    0100 .... = Version: 4
```

C and D) Source address 10.20.0.1 is UA on LTE; destination address of 10.20.0.2 is CS on LTE



```
udp.port == 51102

No.    Time                Source              Destination         Protocol   Lengt Info
23054  1639.0542902…       fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   688   Application Data
23062  1639.4292519…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   716   Application Data
23066  1639.5730927…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   197   Application Data

> Frame 23054: 688 bytes on wire (5504 bits), 688 bytes captured (5504 bits) on interface tun2, id 0
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
    0100 .... = Version: 4
```

e) IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR



```
udp.port == 51102

No.    Time                Source              Destination         Protocol   Lengt Info
23054  1639.0542902…       fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   688   Application Data
23062  1639.4292519…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   716   Application Data
23066  1639.5730927…       fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   197   Application Data

> Frame 23062: 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface tun2, id 0
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0111 0011 1001 1110 0111 = Flow Label: 0x739e7
    Payload Length: 656
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::f
    Destination Address: fd00:bbcc:dde0::a
```

A.1.2 TP_CM_002 – User Plane Traffic Mutual Authentication with UA Access to the CS Denied

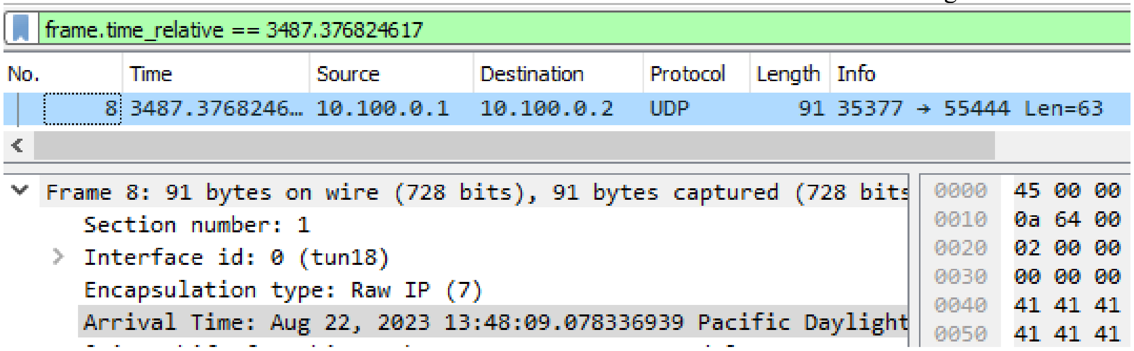
STEP	REQ	Action	Component	Description	Procedure
1	IR-03	VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	lmsf lmsf> status secure Expected Console output: STATUS User: **N**/<ID> | Control: **N**/<ID>

```
2023-08-22 20:47:52.152545  Secure Link Detailed Status:
2023-08-22 20:47:52.152545       userOut enabled: 0
2023-08-22 20:47:52.152545        controlOut enabled: 0
2023-08-22 20:47:52.152545        user plane: NOT CONNECTED
2023-08-22 20:47:52.152545        control plane: NOT CONNECTED
```

2	IR-03	VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	cs-sh lmsf lmsf> status secure Expected output: STATUS User: **N**/<ID> | Control: **N**/<ID>

```
2023-08-22 20:47:45.071307 Secure Link Detailed Status:
2023-08-22 20:47:45.071307      userOut enabled: 0
2023-08-22 20:47:45.071307      controlOut enabled: 0
2023-08-22 20:47:45.071307      user plane: NOT CONNECTED
2023-08-22 20:47:45.071307      control plane: NOT CONNECTED
```

3	IR-03	SEND	UA User Sniffer	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 13:48



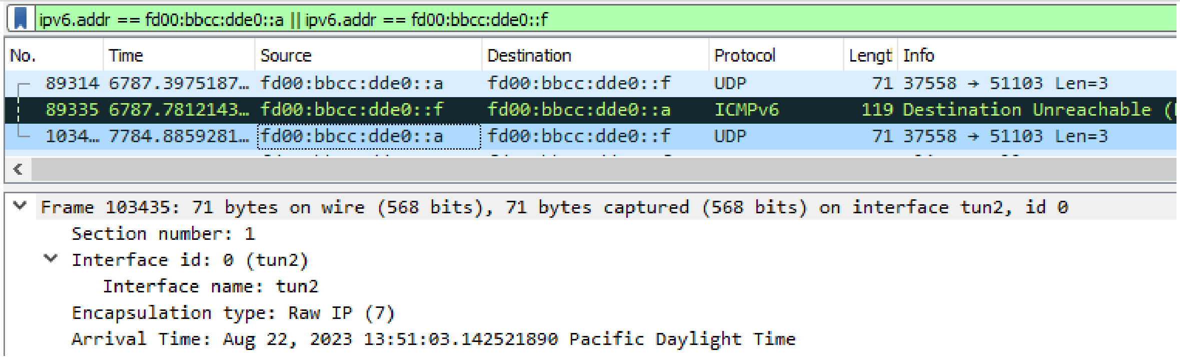
frame.time_relative == 3487.376824617

```
No.   Time           Source       Destination   Protocol  Length  Info
    8 3487.3768246… 10.100.0.1   10.100.0.2    UDP           91  35377 → 55444 Len=63
```

```
Frame 8: 91 bytes on wire (728 bits), 91 bytes captured (728 bits      0000  45 00 00
    Section number: 1                                                  0010  0a 64 00
  > Interface id: 0 (tun18)                                            0020  02 00 00
    Encapsulation type: Raw IP (7)                                     0030  00 00 00
    Arrival Time: Aug 22, 2023 13:48:09.078336939 Pacific Daylight     0040  41 41 41
                                                                       0050  41 41 41
```

4	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	The traffic sniffer log shows that User Data message was not sent by the UA DTSR at time 13:48

STEP	REQ	Action	Component	Description	Procedure

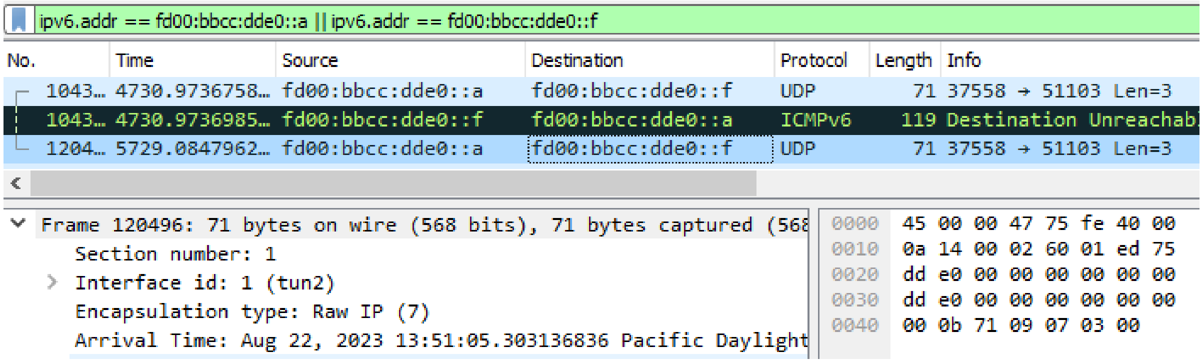


```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time            Source              Destination         Protocol  Lengt Info
89314 6787.3975187… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP        71 37558 → 51103 Len=3
89335 6787.7812143… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  ICMPv6    119 Destination Unreachable (
1034… 7784.8859281… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP        71 37558 → 51103 Len=3

Frame 103435: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 0
    Section number: 1
  Interface id: 0 (tun2)
      Interface name: tun2
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 13:51:03.142521890 Pacific Daylight Time
```

Or, we use the UA DTSR log:

```
2023-08-22 20:48:09.079004 GMT   SessionManager.cpp:293
Sending "ID: 00000008 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue

2023-08-22 20:48:09.079042 GMT INFO     SessionManager.cpp:306
Sent "ID: 00000008 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000008 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	The traffic sniffer log shows that User Data message was not received by the CS DTSR at 13:48



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.    Time            Source              Destination         Protocol  Length Info
1043… 4730.9736758… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP         71 37558 → 51103 Len=3
1043… 4730.9736985… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  ICMPv6     119 Destination Unreachab
1204… 5729.0847962… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP         71 37558 → 51103 Len=3

Frame 120496: 71 bytes on wire (568 bits), 71 bytes captured (568     0000  45 00 00 47 75 fe 40 00
    Section number: 1                                                 0010  0a 14 00 02 60 01 ed 75
  Interface id: 1 (tun2)                                              0020  dd e0 00 00 00 00 00 00
    Encapsulation type: Raw IP (7)                                    0030  dd e0 00 00 00 00 00 00
    Arrival Time: Aug 22, 2023 13:51:05.303136836 Pacific Daylight    0040  00 0b 71 09 07 03 00
```

6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links at CS	`lmsf`
					`lmsf> status 1`
					`Status 2`

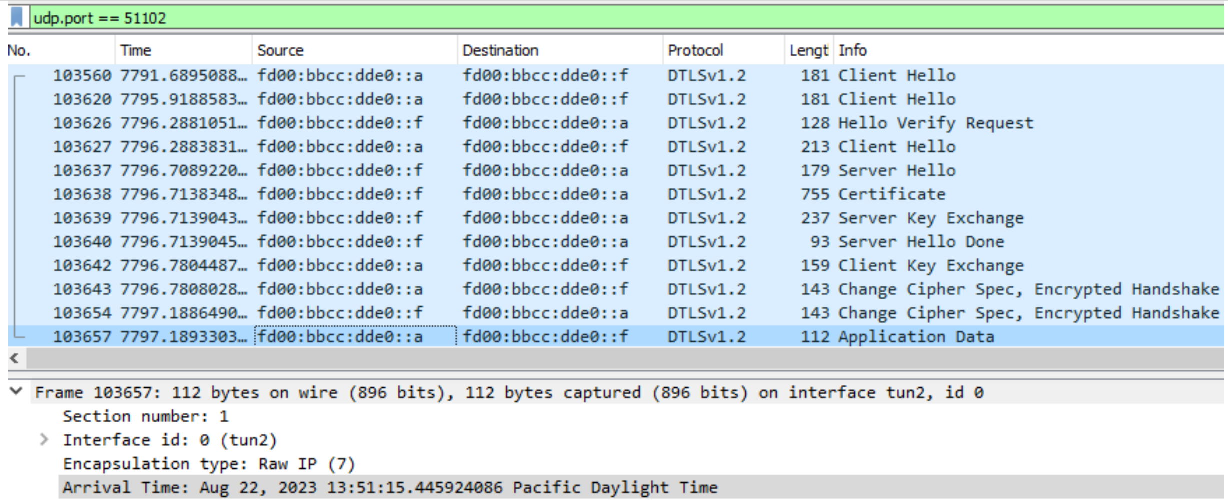
7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	`cs-sh lmsf`
					`lmsf> status 1`
					`status 2`

8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	`cs-sh lmsf`
					`lmsf> secure start`

```
2023-08-22 20:51:04.143057 GMT INFO     ControlOut.cpp:193
Enabling secure session
```

9	IR-01	OBSERVE	CS Main Sniffer	Secure session establishment messages are exchanged over the selected link	Observe secure session establishment messages exchanged

STEP	REQ	Action	Component	Description	Procedure



```
udp.port == 51102

No.     Time           Source              Destination         Protocol   Lengt Info
103560 7791.6895088… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    181 Client Hello
103620 7795.9188583… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    181 Client Hello
103626 7796.2881051… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    128 Hello Verify Request
103627 7796.2883831… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    213 Client Hello
103637 7796.7089220… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    179 Server Hello
103638 7796.7138348… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    755 Certificate
103639 7796.7139043… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    237 Server Key Exchange
103640 7796.7139045… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2     93 Server Hello Done
103642 7796.7804487… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    159 Client Key Exchange
103643 7796.7808028… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    143 Change Cipher Spec, Encrypted Handshake
103654 7797.1886490… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    143 Change Cipher Spec, Encrypted Handshake
103657 7797.1893303… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    112 Application Data

Frame 103657: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 13:51:15.445924086 Pacific Daylight Time
```

From the UA DTSR log:

```
2023-08-22 20:51:15.850216 GMT INFO     ControlIn.cpp:42
Received "DENY_CONNECT 3   " over secure session
Received DENY_CONNECT
Secure connection DENIED by remote peer.
```

10	SER-07
	IR-07
		VERIFY	CS LMSF Console	CS status shows <u>no</u> secure connection for User Plane traffic since UA access to the CS is denied	`Lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: `**`N`**`/<ID> | Control: `**`N`**`/<ID>`

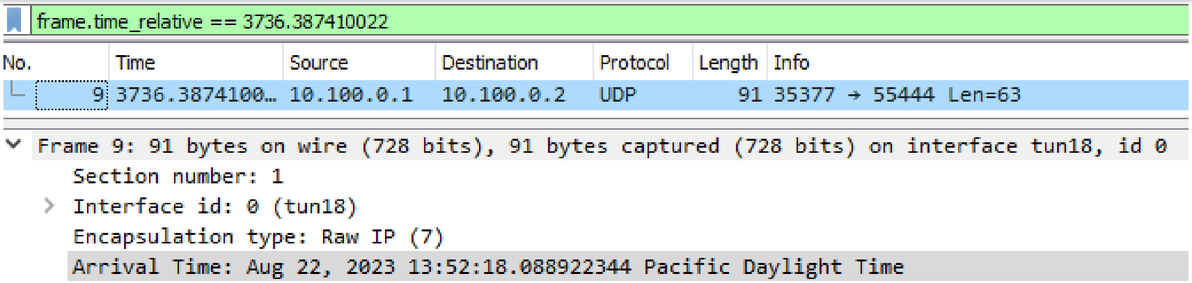
```
From the CS DTSR log:
2023-08-22 20:51:58.067715 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 0
user plane: PENDING PEER
control plane: NOT CONNECTED
```

11	SER-07
	IR-07
		VERIFY	UA LMSF Console	UA status shows <u>no</u> secure connection for User Plane traffic since UA access to the CS is denied	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: `**`N`**`/<ID> | Control: `**`N`**`/<ID>`

```
UA DTSR log:
2023-08-22 20:52:07.992178 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 0
user plane: PENDING PEER
control plane: NOT CONNECTED
```

12	IR-03	SEND	UA UDMD Console	Send User Data	UA User Sniffer shows n=1 message sent to DTSR at 13:52:18

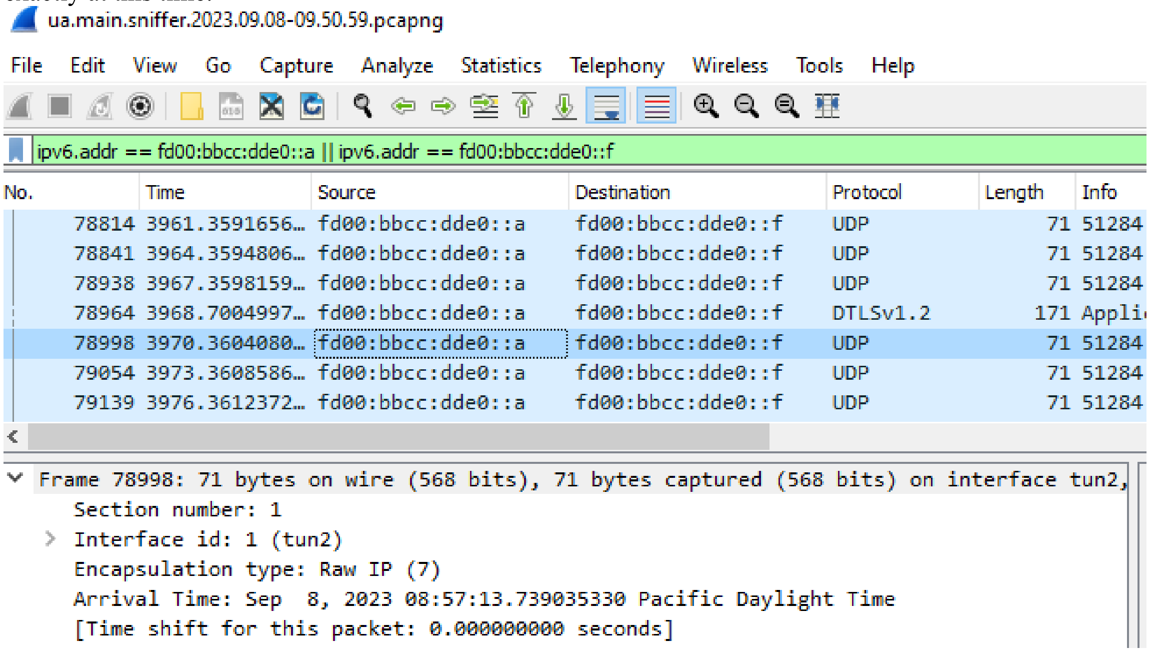
STEP	REQ	Action	Component	Description	Procedure



```
frame.time_relative == 3736.387410022

No.   Time              Source        Destination   Protocol  Length  Info
   9  3736.3874100…     10.100.0.1    10.100.0.2    UDP           91  35377 → 55444 Len=63

Frame 9: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 13:52:18.088922344 Pacific Daylight Time
```

13	IR-03	VERIFY	UA Main Sniffer	User Data is <u>not</u> sent by the UA	The traffic sniffer log shows that User Data message was not sent by the UA DTSR.

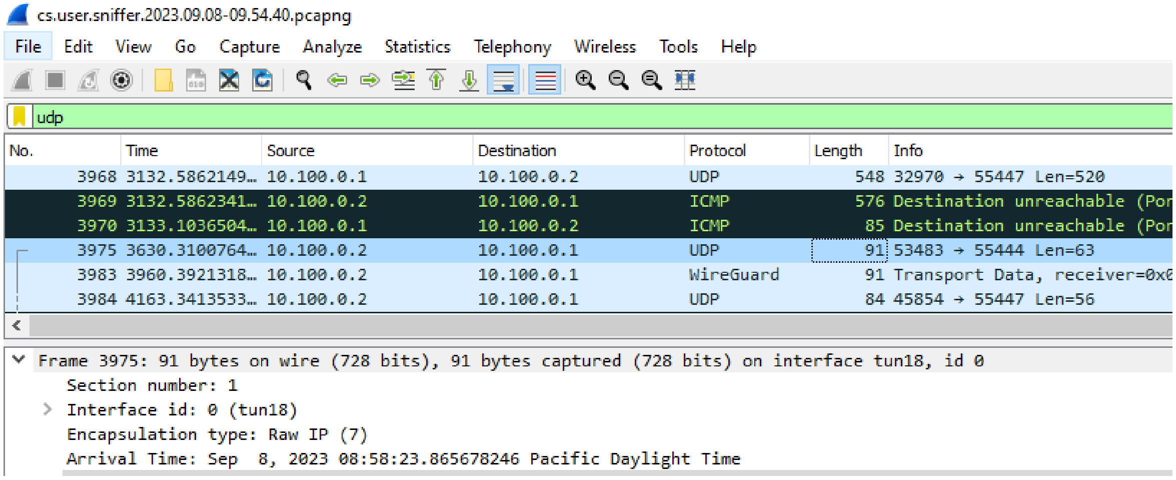
Example from Sept 8th, where the UA Main sniffer shows no matching UDP message at the expected time (08:57:12) when the UDMD tried to send n=1. There are UDP messages before and after this time but not exactly at this time.



ua.main.sniffer.2023.09.08-09.50.59.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.    Time            Source             Destination        Protocol   Length  Info
78814  3961.3591656…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284
78841  3964.3594806…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284
78938  3967.3598159…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284
78964  3968.7004997…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      171  Appli
78998  3970.3604080…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284
79054  3973.3608586…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284
79139  3976.3612372…   fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  UDP            71  51284

Frame 78998: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2,
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 08:57:13.739035330 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
```

14	IR-03	VERIFY	CS User Sniffer	User Data is <u>not</u> received by the CS	The traffic sniffer log shows the User Data message was not received by the CS DTSR



cs.user.sniffer.2023.09.08-09.54.40.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp

No.   Time            Source      Destination  Protocol   Length  Info
3968  3132.5862149…   10.100.0.1  10.100.0.2   UDP           548  32970 → 55447 Len=520
3969  3132.5862341…   10.100.0.2  10.100.0.1   ICMP          576  Destination unreachable (Por
3970  3133.1036504…   10.100.0.1  10.100.0.2   ICMP           85  Destination unreachable (Por
3975  3630.3100764…   10.100.0.2  10.100.0.1   UDP            91  53483 → 55444 Len=63
3983  3960.3921318…   10.100.0.2  10.100.0.1   WireGuard      91  Transport Data, receiver=0x0
3984  4163.3413533…   10.100.0.2  10.100.0.1   UDP            84  45854 → 55447 Len=56

Frame 3975: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 08:58:23.865678246 Pacific Daylight Time
```

CS User sniffer shows no UDP message at 08:57:12 when the message from the UA was attempted.

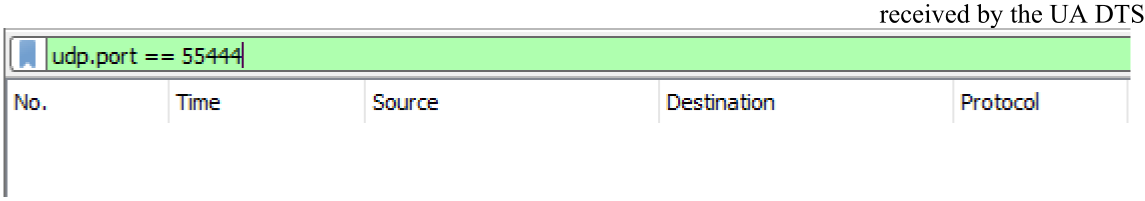
STEP	REQ	Action	Component	Description	Procedure

15	IR-03	SEND	CS UDMD Console	Send User Data	`udmd`
					`udmd> send n=1`

16	IR-03	VERIFY	CS Main Sniffer	User Data is <u>not</u> sent by the CS	The traffic sniffer log shows that User Data message was not sent by the CS DTSR at time

The expected result is to see an error message in the DTSR log indicating the message cannot be sent. The CS Main sniffer should show no message at the instant the n=1 was attempted. None of the test cases passed for this condition to paste examples.

STEP	REQ	Action	Component	Description	Procedure
17	IR-03	VERIFY	UA Main Sniffer	User Data is <u>not</u> received by the UA	The traffic sniffer log shows the User Data message was not received by the UA DTSR



udp.port == 55444

No.	Time	Source	Destination	Protocol

No messages for port 55444 (user data).

A.1.3 TP_CM_003 – User Plane Traffic Mutual Authentication with CS Access to the UA Denied

STEP	REQ	Action	Component	Description	Procedure

1	IR-03	VERIFY	CS LMSF console	CS status shows <u>no</u> secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User:` **N**`/<ID> | Control:` **N**`/<ID>`

```
2023-08-22 18:23:53.916215 GMT INFO  SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

2	IR-03	VERIFY	UA LMSF console	UA status shows <u>no</u> secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User:` **N**`/<ID> | Control:` **N**`/<ID>`

```
2023-08-22 18:24:00.234683 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

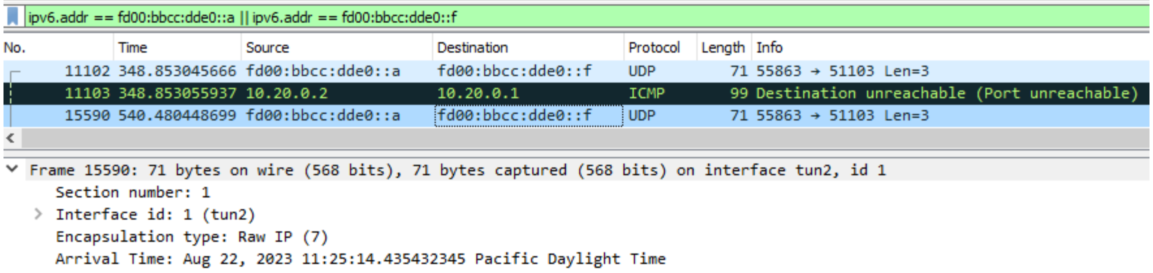
3	IR-03	SEND	UA UDMD Console	Send User Data	`cs-sh udmd`
					`udmd> send n=1 at 18:24 GMT`

4	IR-03	VERIFY	UA Main Sniffer	User Data is <u>not</u> sent by the UA	Verify via the traffic sniffer log that User Data message is not sent by the UA DTSR

STEP	REQ	Action	Component	Description	Procedure

```
2023-08-22 18:24:30.438765 GMT INFO    UdmdIn.cpp:51
Received: ID: 00000002  Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002
Origin: UDMD  Cmd: SEND Size: 63 Rsp: FALSE not sent to peer
Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue Unexpected message type: ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp:
TRUE Sent "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000002
Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE not sent to peer to lmsf_queue
```

5	IR-03	VERIFY	CS Main Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that the User Data message was not received by the CS DTSR at 11:24:30



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time          Source            Destination       Protocol  Length Info
  11102 348.853045666 fd00:bbcc:dde0::a fd00:bbcc:dde0::f UDP           71 55863 → 51103 Len=3
  11103 348.853055937 10.20.0.2         10.20.0.1         ICMP          99 Destination unreachable (Port unreachable)
  15590 540.480448699 fd00:bbcc:dde0::a fd00:bbcc:dde0::f UDP           71 55863 → 51103 Len=3

Frame 15590: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface tun2, id 1
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 11:25:14.435432345 Pacific Daylight Time
```

CS Main sniffer shows message at 11:22, and next message at 11:25:14 (nothing at 11:24:30)

6	IR-08	OBSERVE	CS LMSF Console	View the status of all available links at CS	`lmsf`
					`lmsf> status`

7	IR-08	OBSERVE	UA LMSF Console	View the status of all available links at UA	`cs-sh lmsf`
					`lmsf> status`

8	IR-01	SEND	UA LMSF Console	Establish secure session for the Control Plane and User Plane traffic	`cs-sh lmsf`
					`lmsf> secure start`

```
2023-08-22 18:25:15.273392 GMT INFO     ControlOut.cpp:193
Enabling secure session
```

9	IR-01	OBSERVE	CS Main Sniffer	Secure session establishment are exchanged over the selected link	Observe secure session establishment messages exchanged

10	SER-07
	IR-07
		VERIFY	CS LMSF Console	CS status shows no secure connection for User Plane traffic since CS access to the UA is denied	`lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User:` **N**`/<ID> |`
					`Control:` **N**`/<ID>`

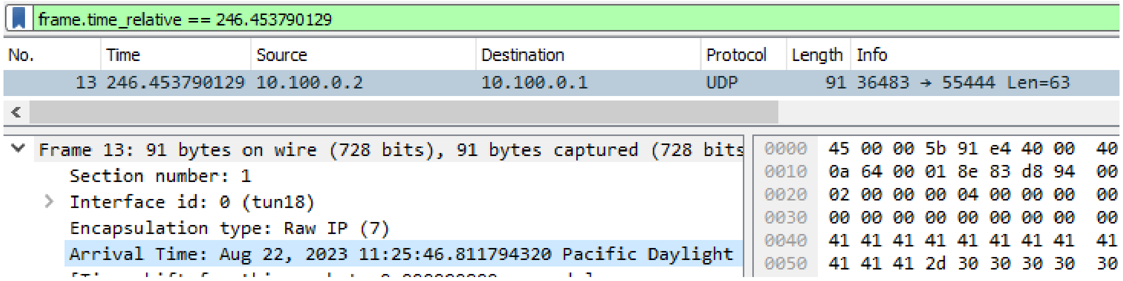
```
2023-08-22 18:25:32.068847 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

11	SER-07
	IR-07
		VERIFY	UA LMSF Console	UA status shows no secure connection for User Plane traffic since CS access to the UA is denied	`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: N/<ID> | Control: N/<ID>`

```
2023-08-22 18:25:37.654528 GMT INFO     SessionManager.cpp:330
Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

12	IR-03	SEND	CS UDMD Console	Send User Data	`udmd`
					`udmd> send n=1`



```
frame.time_relative == 246.453790129

No.  Time          Source      Destination  Protocol  Length  Info
  13 246.453790129 10.100.0.2  10.100.0.1   UDP           91  36483 → 55444 Len=63

Frame 13: 91 bytes on wire (728 bits), 91 bytes captured (728 bits
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 11:25:46.811794320 Pacific Daylight

0000  45 00 00 5b 91 e4 40 00  40
0010  0a 64 00 01 8e 83 d8 94  00
0020  02 00 00 00 04 00 00 00  00
0030  00 00 00 00 00 00 00 00  00
0040  41 41 41 41 41 41 41 41  41
0050  41 41 41 2d 30 30 30 30  30
```

```
CS User sniffer shows UDMD message at 11:25:46 PDT
```

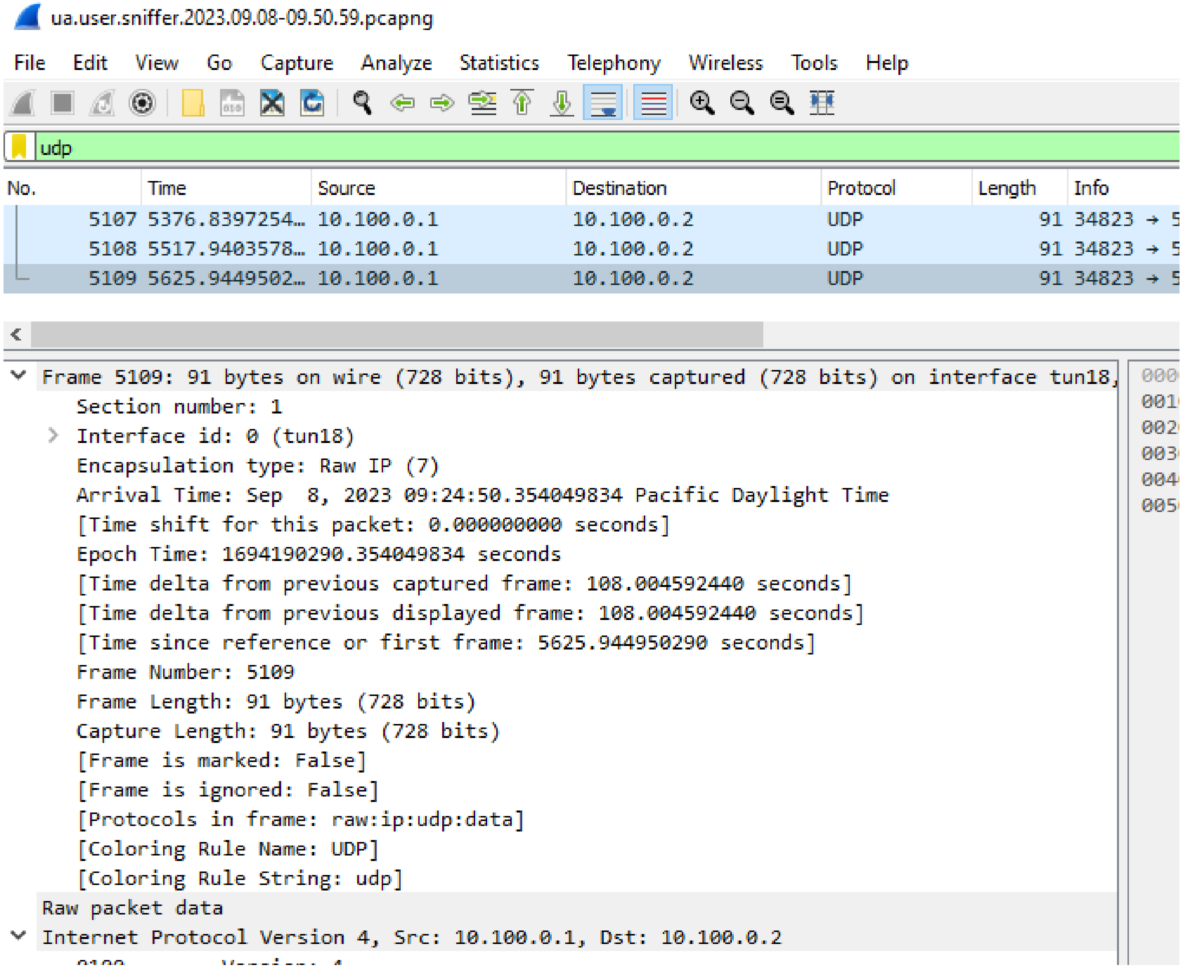
13	IR-03	VERIFY	CS Main Sniffer	User Data is not sent by the CS	The traffic sniffer log shows that User Data message was not sent by the CS DTSR at time 18:25:46 GMT

```
2023-08-22 18:25:46.811837 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data:UD-AAAAAAAAAAAAAAAAAAA-000002
Sending user data message to peer
Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer
Sending "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue
Sent "ID: 00000002 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000002 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

14	IR-03	VERIFY	UA User Sniffer Log	User Data is not received by the UA	Verify via the traffic sniffer log that that no User Data message was received by the UA DTSR

STEP	REQ	Action	Component	Description	Procedure

Example from test on Sept 8th. CS sent n=1 at 9:24:21; UA User Sniffer shows no messages received at that time with source 10.100.0.2.



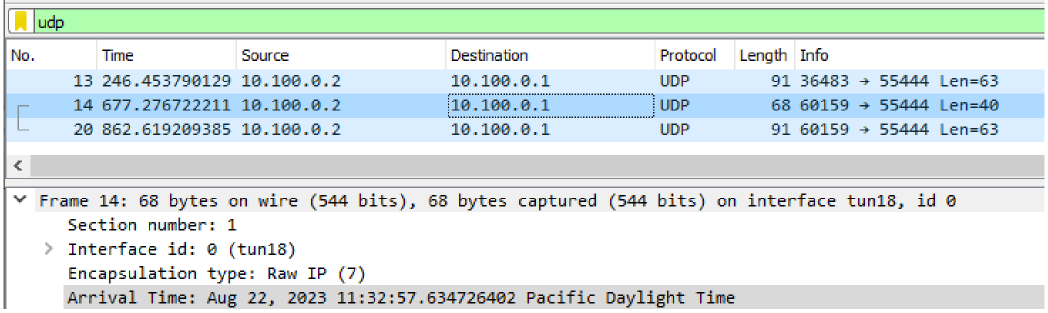
```
No.        Time             Source       Destination   Protocol  Length  Info
     5107 5376.8397254… 10.100.0.1   10.100.0.2    UDP          91 34823 → 5
     5108 5517.9403578… 10.100.0.1   10.100.0.2    UDP          91 34823 → 5
     5109 5625.9449502… 10.100.0.1   10.100.0.2    UDP          91 34823 → 5

Frame 5109: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18,
   Section number: 1
 > Interface id: 0 (tun18)
   Encapsulation type: Raw IP (7)
   Arrival Time: Sep  8, 2023 09:24:50.354049834 Pacific Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1694190290.354049834 seconds
   [Time delta from previous captured frame: 108.004592440 seconds]
   [Time delta from previous displayed frame: 108.004592440 seconds]
   [Time since reference or first frame: 5625.944950290 seconds]
   Frame Number: 5109
   Frame Length: 91 bytes (728 bits)
   Capture Length: 91 bytes (728 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: raw:ip:udp:data]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Raw packet data
Internet Protocol Version 4, Src: 10.100.0.1, Dst: 10.100.0.2
```

15	IR-03	SEND	UA UDMD Console	Send User Data	udmd udmd> send n=1
16	IR-03	VERIFY	UA Main Sniffer	User Data is not sent by the UA	Notification that User Data cannot be sent from the UA DTSR

```
2023-08-22 18:25:57.442190 GMT INFO      UdmdIn.cpp:51
Received: ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data:UD-AAAAAAAAAAAAAAAAAAA-000004
Sending user data message to peer
Secure session disabled - ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer
Sending "ID: 00000004 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: " to lmsf_queue
Sent "ID: 00000004 Origin: UDMD Cmd: SEND Size: 136 Rsp: TRUE Success: F
Msg: Secure session disabled - ID: 00000004 Origin: UDMD Cmd: SEND Size: 63
Rsp: FALSE not sent to peer to lmsf_queue
```

17	IR-03	VERIFY	CS User Sniffer	User Data is not received by the CS	Verify via the traffic sniffer log that no User Data message was received by the CS DTSR or UDMD

STEP	REQ	Action	Component	Description	Procedure



```
udp
No.    Time          Source      Destination  Protocol  Length  Info
    13 246.453790129 10.100.0.2  10.100.0.1   UDP           91  36483 → 55444 Len=63
    14 677.276722211 10.100.0.2  10.100.0.1   UDP           68  60159 → 55444 Len=40
    20 862.619209385 10.100.0.2  10.100.0.1   UDP           91  60159 → 55444 Len=63

Frame 14: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 22, 2023 11:32:57.634726402 Pacific Daylight Time
```

CS User Sniffer shows UDP message at 11:25:46 PDT and the next message is 11:32:57, which is the next scenario. Nothing at 11:25 or 11:26 when UDMD would expect to receive it.

A.1.4 TP_CM_004 – User Data Exchanges with Encryption

A.1.4.1 TP_CM_004A – USER DATA EXCHANGES WITH ENCRYPTION, PAYLOAD DATA < MTU

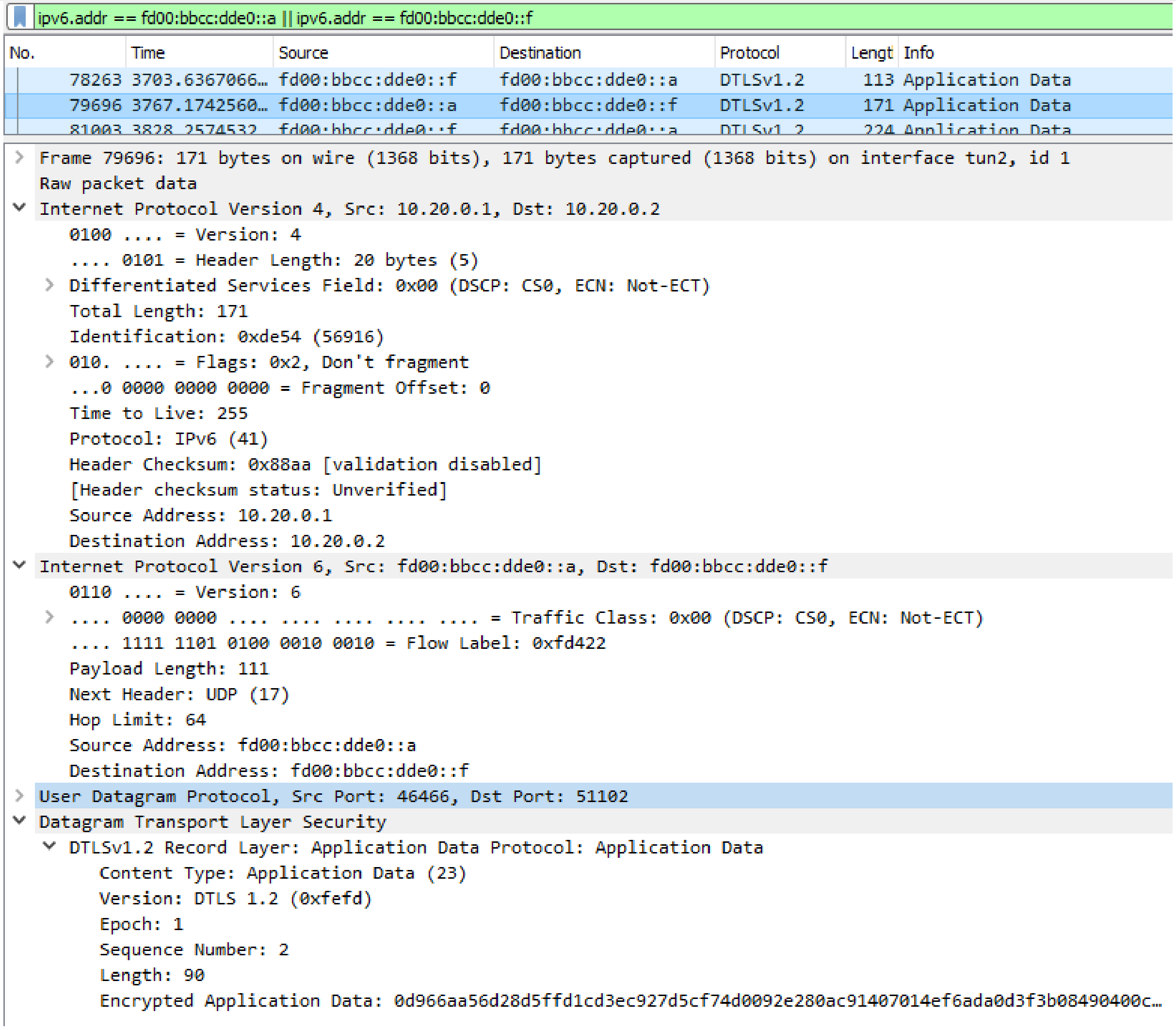
STEP	REQ	Action	Component	Description	Procedure

1	IR-09b	SEND	UA UDMD Console	Send a User Data less than MTU size	`udmd`
					`udmd> send n=1`

```
UA DTSR
2023-08-24 16:57:31.818437 GMT INFO      UdmdIn.cpp:51
Received: ID: 00000004 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAA-000004
Sending user data message to peer
User Output: Sent 66 bytes.
Buffer Contents: [0542000400000002  000000040000007f  0000003f00000000
00000000fa107455 00000055442d4141  4141414141414141  4141414141414141
41412d3030303030  3400]
Sent "USER_DATA.REQ           66
```

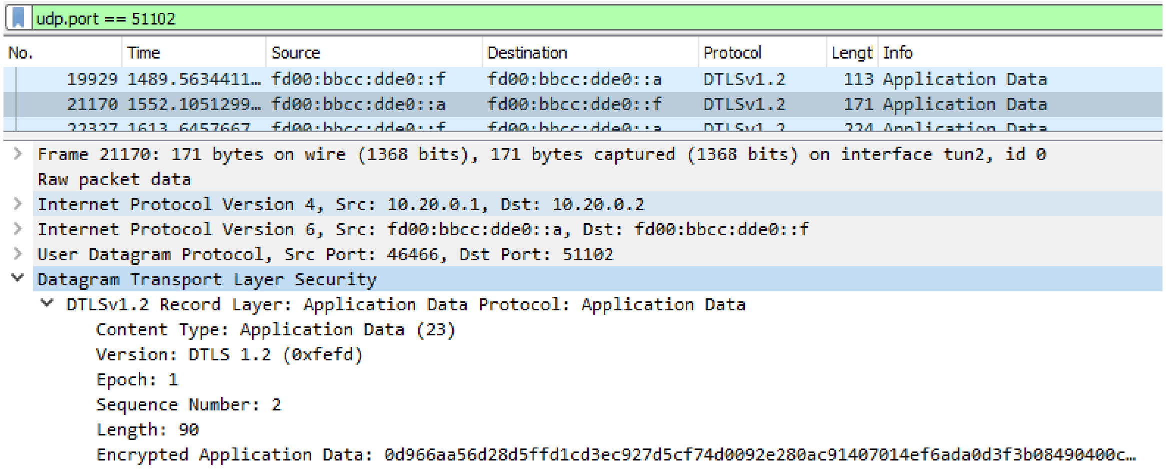
STEP	REQ	Action	Component	Description	Procedure
2	IR-09b	VERIFY	CS Main Sniffer	User Data < MTU does not require segmentation	Verify via the traffic sniffer log that User Data was not segmented

STEP	REQ	Action	Component	Description	Procedure



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time              Source              Destination         Protocol   Lengt Info
  78263 3703.6367066…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   113 Application Data
  79696 3767.1742560…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   171 Application Data
  81003 3828.2574532      fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data

> Frame 79696: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 171
    Identification: 0xde54 (56916)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: IPv6 (41)
    Header Checksum: 0x88aa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.20.0.1
    Destination Address: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1111 1101 0100 0010 0010 = Flow Label: 0xfd422
    Payload Length: 111
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 2
      Length: 90
      Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

3	SER-04	VERIFY	UA Main Sniffer	User Data sent is encrypted	Verify via the traffic sniffer log that the content of the User Data message sent cannot be discerned

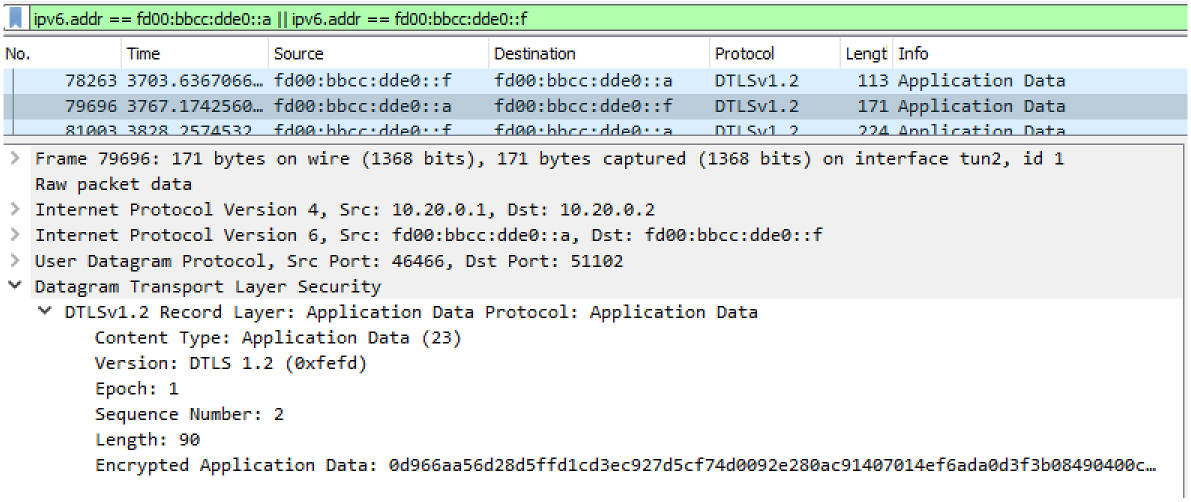


```
udp.port == 51102

No.     Time              Source              Destination         Protocol   Lengt Info
  19929 1489.5634411…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   113 Application Data
  21170 1552.1051299…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   171 Application Data
  22327 1613.6457667      fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data

> Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 0
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 2
      Length: 90
      Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

UA Main sniffer shows application data is encrypted

4	SER-04	VERIFY	CS Main Sniffer	User Data received is encrypted	Verify via the traffic sniffer log that the content of the User Data message received cannot be discerned

STEP	REQ	Action	Component	Description	Procedure



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time              Source              Destination         Protocol   Lengt Info
  78263 3703.6367066…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2     113 Application Data
  79696 3767.1742560…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2     171 Application Data
  81003 3828.2574532   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2     224 Application Data

> Frame 79696: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 1
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
   v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
        Content Type: Application Data (23)
        Version: DTLS 1.2 (0xfefd)
        Epoch: 1
        Sequence Number: 2
        Length: 90
        Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

CS Main Sniffer shows application data is encrypted

Post-test Log Analysis

5	SER-02 SER-04	VERIFY	CS and UA DTSR Live Log	User Data received matches User Data sent which indicates the message was accepted as authentic.	a) Compare the CS DTSR log with the source data on the UA to show that the sent and received contents are the same b) Compare the UA DTSR log with the source data on the CS to show that the sent and received contents are the same.

UA DTSR

```
2023-08-24 16:57:31.818437 GMT INFO     UdmdIn.cpp:51
Sending user data message to peer
User Output: Sent 66 bytes.
Buffer Contents: [0542000400000002  000000040000007f  0000003f00000000
00000000fa107455 00000055442d4141  4141414141414141  4141414141414141
41412d3030303030  3400]
```

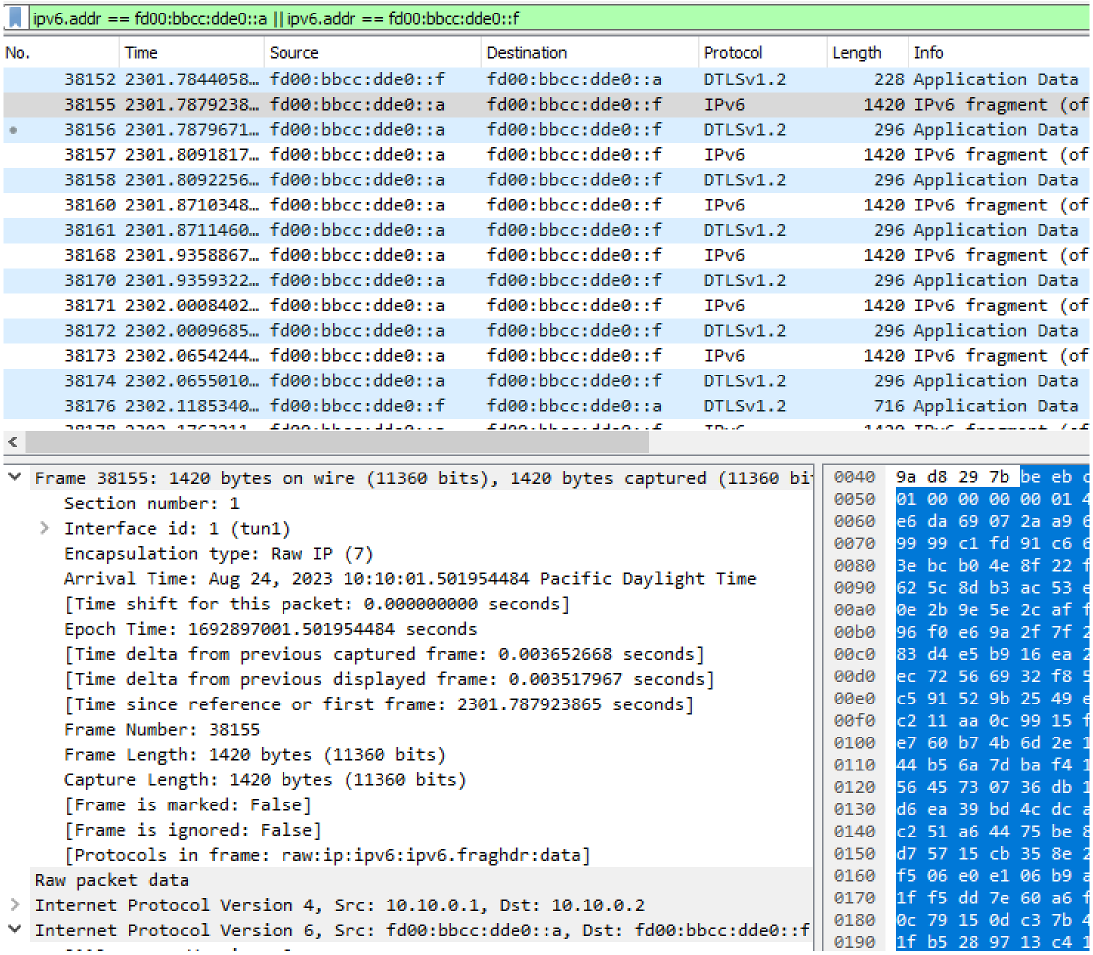
CS DTSR

```
2023-08-24 16:57:31.977458 GMT INFO     UserIn.cpp:43
Received "USER_DATA.REQ           66
0542000400000002  000000040000007f  0000003f00000000 00000000fa107455
00000055442d4141  4141414141414141  4141414141414141  41412d3030303030  3400
```

A.1.4.2 TP_CM_004B – USER DATA EXCHANGES WITH ENCRYPTION, PAYLOAD DATA > MTU

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	CS OS Console	Send a User Data greater than MTU size	`cs-rft <filename> <local filename>`
2	IR-09b	VERIFY	UA Main Sniffer	User Data > MTU is segmented	Verify via the traffic sniffer log that User Data was segmented

STEP	REQ	Action	Component	Description	Procedure



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time           Source             Destination        Protocol   Length Info
  38152 2301.7844058… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      228 Application Data
  38155 2301.7879238… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38156 2301.7879671… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38157 2301.8091817… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38158 2301.8092256… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38160 2301.8710348… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38161 2301.8711460… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38168 2301.9358867… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38170 2301.9359322… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38171 2302.0008402… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38172 2302.0009685… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38173 2302.0654244… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
  38174 2302.0655010… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      296 Application Data
  38176 2302.1185340… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      716 Application Data
  38178 2302.1763211… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6         1420 IPv6 fragment (of
```

```
v Frame 38155: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bi      0040  9a d8 29 7b be eb c
      Section number: 1                                                             0050  01 00 00 00 00 01 4
    > Interface id: 1 (tun1)                                                        0060  e6 da 69 07 2a a9 6
      Encapsulation type: Raw IP (7)                                                0070  99 99 c1 fd 91 c6 6
      Arrival Time: Aug 24, 2023 10:10:01.501954484 Pacific Daylight Time           0080  3e bc b0 4e 8f 22 f
      [Time shift for this packet: 0.000000000 seconds]                             0090  62 5c 8d b3 ac 53 e
      Epoch Time: 1692897001.501954484 seconds                                      00a0  0e 2b 9e 5e 2c af f
      [Time delta from previous captured frame: 0.003652668 seconds]                00b0  96 f0 e6 9a 2f 7f 2
      [Time delta from previous displayed frame: 0.003517967 seconds]               00c0  83 d4 e5 b9 16 ea 2
      [Time since reference or first frame: 2301.787923865 seconds]                 00d0  ec 72 56 69 32 f8 5
      Frame Number: 38155                                                           00e0  c5 91 52 9b 25 49 e
      Frame Length: 1420 bytes (11360 bits)                                         00f0  c2 11 aa 0c 99 15 f
      Capture Length: 1420 bytes (11360 bits)                                       0100  e7 60 b7 4b 6d 2e 1
      [Frame is marked: False]                                                      0110  44 b5 6a 7d ba f4 1
      [Frame is ignored: False]                                                     0120  56 45 73 07 36 db 1
      [Protocols in frame: raw:ip:ipv6:ipv6.fraghdr:data]                           0130  d6 ea 39 bd 4c dc a
  Raw packet data                                                                   0140  c2 51 a6 44 75 be 8
> Internet Protocol Version 4, Src: 10.10.0.1, Dst: 10.10.0.2                       0150  d7 57 15 cb 35 8e 2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f       0160  f5 06 e0 e1 06 b9 a
                                                                                    0170  1f f5 dd 7e 60 a6 f
                                                                                    0180  0c 79 15 0d c3 7b 4
                                                                                    0190  1f b5 28 97 13 c4 1
```

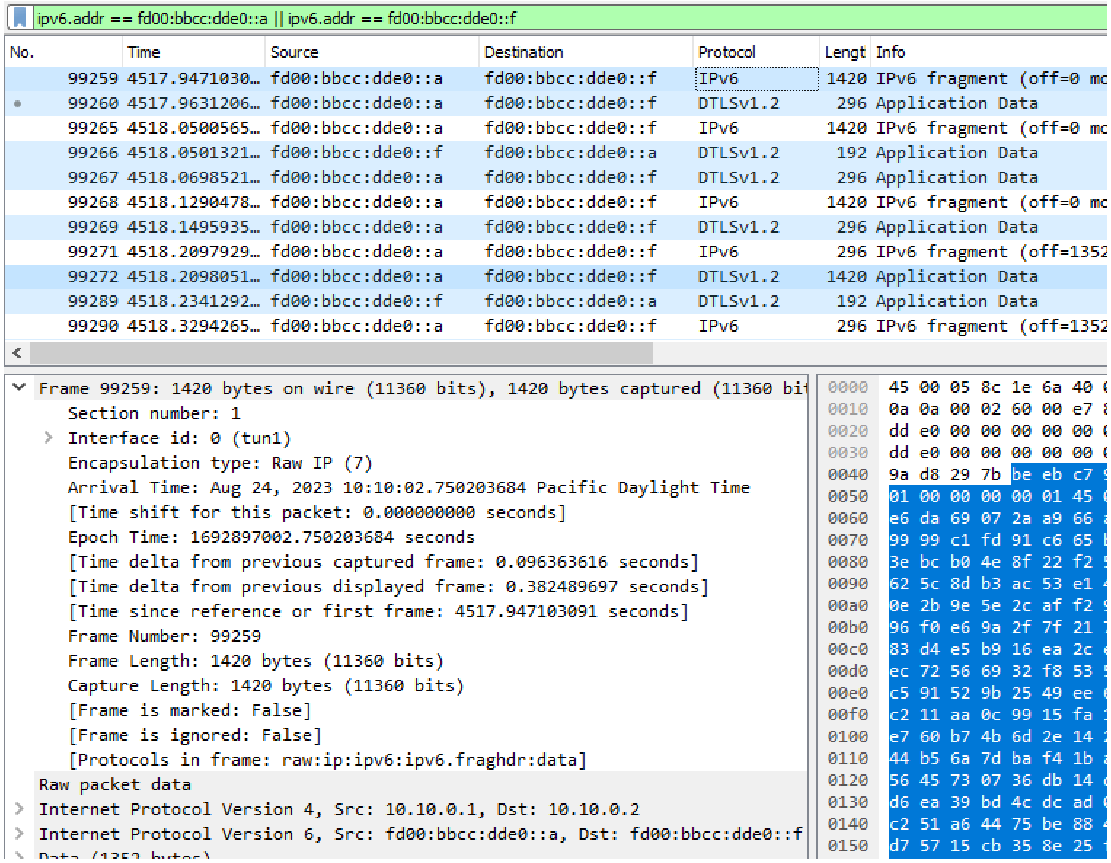
UA Main Sniffer shows messages are divided into max length of 1420 bytes.

3	SER-04	VERIFY	UA Main Sniffer	User Data sent is encrypted	Verify via the traffic sniffer log that the content of the User Data message sent cannot be discerned

UA Main sniffer log snapshot in step 2 shows message is encrypted.

4	SER-04	VERIFY	CS Main Sniffer	User Data received is encrypted	Verify via the traffic sniffer log that the content of the User Data message received cannot be discerned

STEP	REQ	Action	Component	Description	Procedure



```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.     Time             Source             Destination        Protocol  Lengt Info
  99259 4517.9471030…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6      1420 IPv6 fragment (off=0 mc
• 99260 4517.9631206…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   296 Application Data
  99265 4518.0500565…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6      1420 IPv6 fragment (off=0 mc
  99266 4518.0501321…  fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2   192 Application Data
  99267 4518.0698521…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   296 Application Data
  99268 4518.1290478…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6      1420 IPv6 fragment (off=0 mc
  99269 4518.1495935…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   296 Application Data
  99271 4518.2097929…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6       296 IPv6 fragment (off=1352
  99272 4518.2098051…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2  1420 Application Data
  99289 4518.2341292…  fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2   192 Application Data
  99290 4518.3294265…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  IPv6       296 IPv6 fragment (off=1352
```

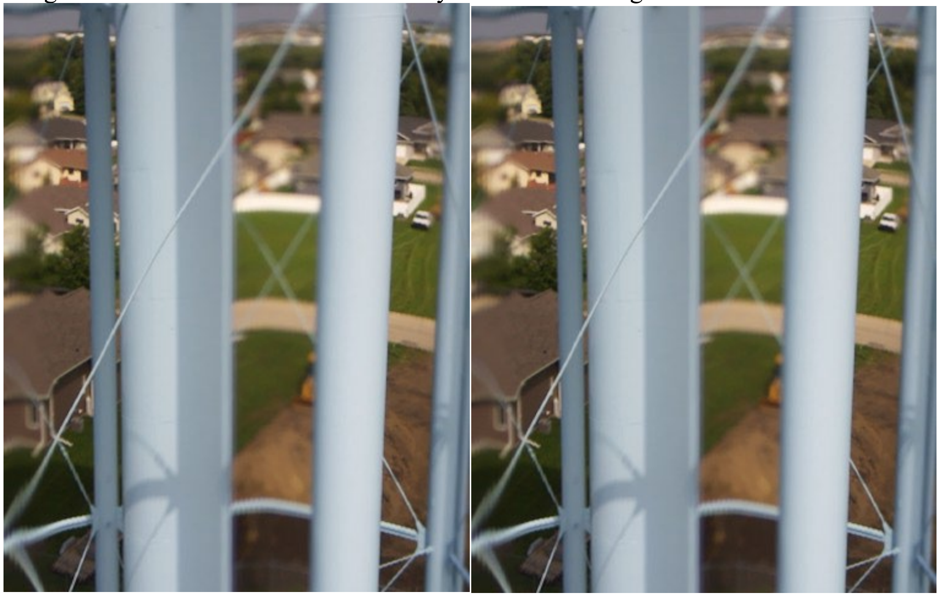
```
v Frame 99259: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bit      0000  45 00 05 8c 1e 6a 40
     Section number: 1                                                               0010  0a 0a 00 02 60 00 e7
   > Interface id: 0 (tun1)                                                          0020  dd e0 00 00 00 00 00
     Encapsulation type: Raw IP (7)                                                  0030  dd e0 00 00 00 00 00
     Arrival Time: Aug 24, 2023 10:10:02.750203684 Pacific Daylight Time             0040  9a d8 29 7b be eb c7
     [Time shift for this packet: 0.000000000 seconds]                               0050  01 00 00 00 00 01 45
     Epoch Time: 1692897002.750203684 seconds                                        0060  e6 da 69 07 2a a9 66
     [Time delta from previous captured frame: 0.096363616 seconds]                  0070  99 99 c1 fd 91 c6 65
     [Time delta from previous displayed frame: 0.382489697 seconds]                 0080  3e bc b0 4e 8f 22 f2
     [Time since reference or first frame: 4517.947103091 seconds]                   0090  62 5c 8d b3 ac 53 e1
     Frame Number: 99259                                                             00a0  0e 2b 9e 5e 2c af f2
     Frame Length: 1420 bytes (11360 bits)                                           00b0  96 f0 e6 9a 2f 7f 21
     Capture Length: 1420 bytes (11360 bits)                                         00c0  83 d4 e5 b9 16 ea 2c
     [Frame is marked: False]                                                        00d0  ec 72 56 69 32 f8 53
     [Frame is ignored: False]                                                       00e0  c5 91 52 9b 25 49 ee
     [Protocols in frame: raw:ip:ipv6:ipv6.fraghdr:data]                             00f0  c2 11 aa 0c 99 15 fa
  Raw packet data                                                                    0100  e7 60 b7 4b 6d 2e 14
> Internet Protocol Version 4, Src: 10.10.0.1, Dst: 10.10.0.2                        0110  44 b5 6a 7d ba f4 1b
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f        0120  56 45 73 07 36 db 14
                                                                                     0130  d6 ea 39 bd 4c dc ad
                                                                                     0140  c2 51 a6 44 75 be 88
                                                                                     0150  d7 57 15 cb 35 8e 25
```

CS Main sniffer shows messages are encrypted

Post-test Log Analysis

5	SER-02 SER-04	VERIFY	UA and CS Content Directory	User Data received matches User Data sent which indicates the message was accepted as authentic.	Compare the received User Data file with the source User Data file on the UA to show that the sent and received contents are the same

Image sent from the UA content directory matches the image downloaded from cloud.



A.1.5 TP_CM_005 – User Data Exchanges without Encryption

A.1.5.1 TP_CM_005A – USER DATA EXCHANGES WITHOUT ENCRYPTION, PAYLOAD DATA < MTU

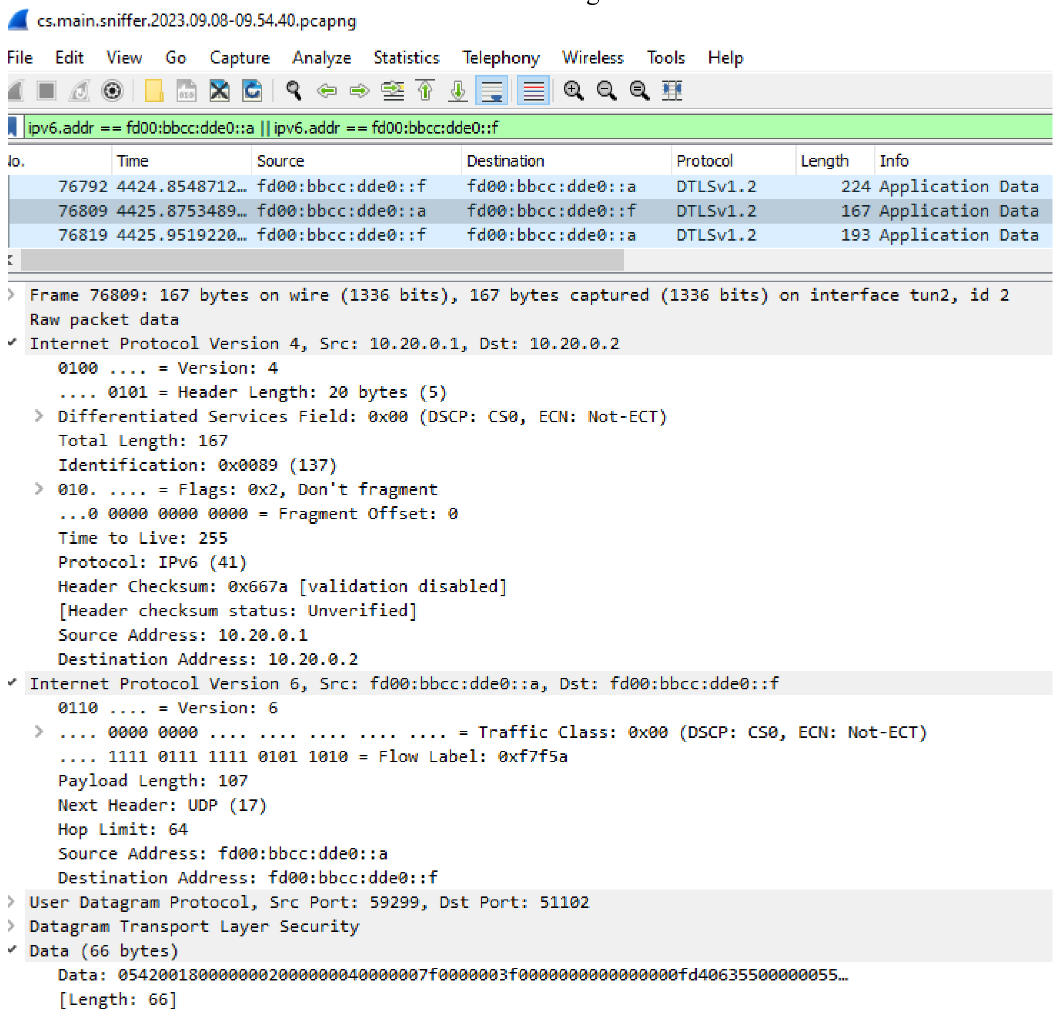
Procedure:

STEP	REQ	Action	Component	Description	Procedure

1	IR-09b	SEND	UA UDMD Console	Send User Data less than MTU size	`cs-sh`
					`udmd> send n=1`

```
UA DTSR
2023-09-08 16:08:27.122153 GMT INFO      UdmdIn.cpp:51
Received: ID: 00000024 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE
Data: UD-AAAAAAAAAAAAAAAAAAA-000024
Sending user data message to peer
User Output: Sent 66 bytes.
```

2	IR-09b	VERIFY	CS Main Sniffer	User Data < MTU does not require segmentation	Verify via the traffic sniffer log that User Data was not segmented



ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

```
No.   Time            Source             Destination        Protocol   Length Info
76792 4424.8548712…  fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      224 Application Data
76809 4425.8753489…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      167 Application Data
76819 4425.9519220…  fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      193 Application Data
```

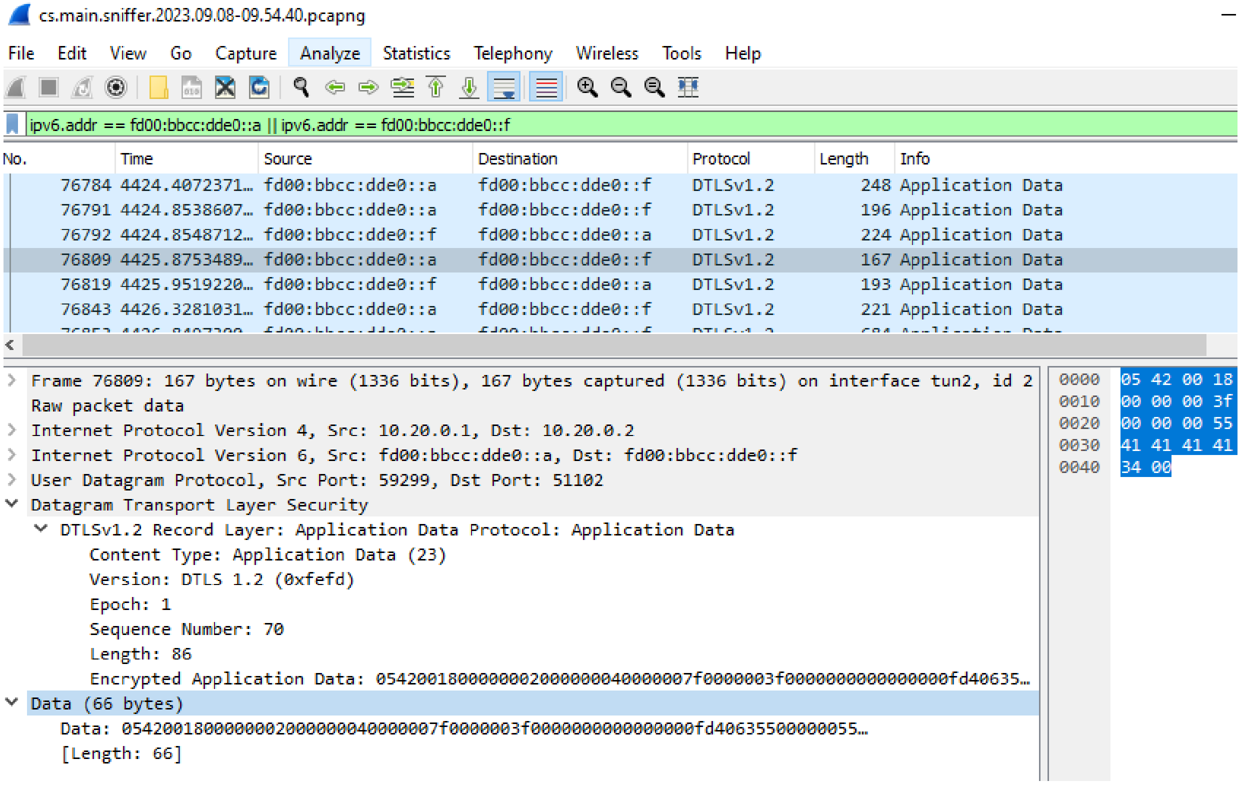
```
> Frame 76809: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface tun2, id 2
  Raw packet data
✓ Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 167
    Identification: 0x0089 (137)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: IPv6 (41)
    Header Checksum: 0x667a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.20.0.1
    Destination Address: 10.20.0.2
✓ Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1111 0111 1111 0101 1010 = Flow Label: 0xf7f5a
    Payload Length: 107
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 59299, Dst Port: 51102
> Datagram Transport Layer Security
✓ Data (66 bytes)
    Data: 0542001800000002000000040000007f0000003f0000000000000000fd40635500000055…
    [Length: 66]
```

3	SER-02	VERIFY	CS and UA DTSR Live Log	User Data received matches User Data sent	Verify the received User Data message has the same contents as the one that was sent

STEP	REQ	Action	Component	Description	Procedure
CS DTSR 2023-09-08 16:08:26.844668 GMT DEBUG InputMessage.cpp:161 Received 66 bytes of data from User Input User Input: Expected message size is 66 bytes User Input Buffer Contents: [0542001800000002 000000040000007f 0000003f00000000 00000000fd406355 00000055442d4141 4141414141414141 4141414141414141 41412d3030303032 3400] Processing USER_DATA.REQ Sent "ID: 00000024 Origin: DTSR-UA Cmd: SEND Size: 63 Rsp: FALSE Data: UD-AAAAAAAAAAAAAAAAAAAA-000024" to udmd_queue					
4	SER-02	VERIFY	CS Main Sniffer	User Data is not encrypted and authentication tag is at least 64 bits	Verify via the traffic sniffer log that: a) User Data is not encrypted (i.e., plaintext data is visible in the log) b) User Data messages contains an authentication tag that's least 64 bits

CS Sniffer log in step 2 shows data is not encrypted; the message is sent in the clear in binary.

b) The payload is 86 bytes long, while the message is only 66 bytes long. The other 20 bytes is the tag. The registered NULL cipher suite invokes the user of HMAC with the SHA-1 hash algorithm which produces a non-truncated 20 byte (160 bit) authentication tag.

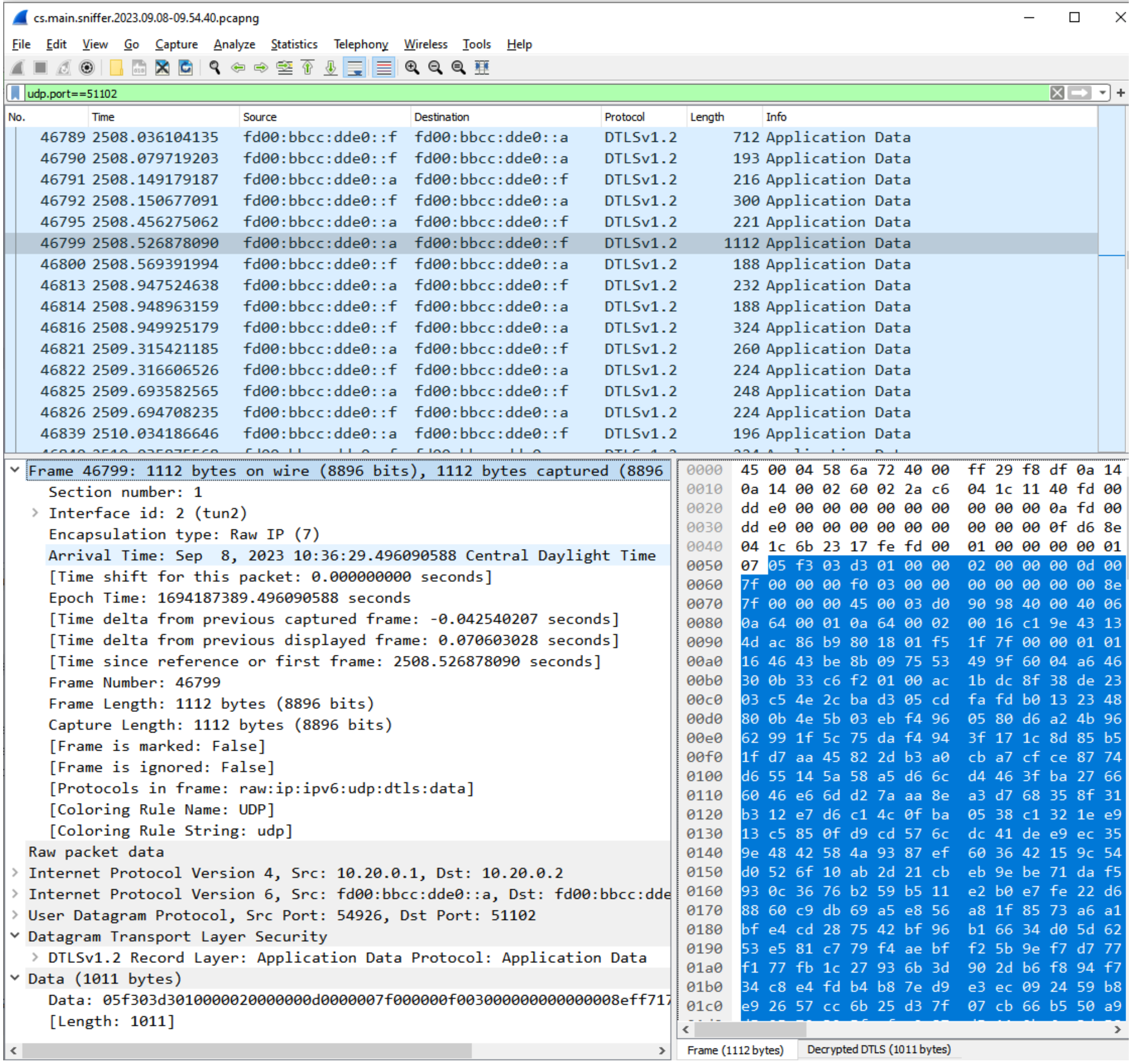


```
ipv6.addr == fd00:bbcc:dde0::a || ipv6.addr == fd00:bbcc:dde0::f

No.   Time            Source              Destination         Protocol   Length Info
76784 4424.4072371…   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   248 Application Data
76791 4424.8538607…   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   196 Application Data
76792 4424.8548712…   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data
76809 4425.8753489…   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   167 Application Data
76819 4425.9519220…   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   193 Application Data
76843 4426.3281031…   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   221 Application Data

> Frame 76809: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface tun2, id 2
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 59299, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 70
      Length: 86
      Encrypted Application Data: 0542001800000002000000040000007f0000003f0000000000000000fd40635…
v Data (66 bytes)
    Data: 0542001800000002000000040000007f0000003f0000000000000000fd40635500000055…
    [Length: 66]

0000  05 42 00 18
0010  00 00 00 3f
0020  00 00 00 55
0030  41 41 41 41
0040  34 00
```

A.1.5.2 TP_CM_005B – USER DATA EXCHANGES WITHOUT ENCRYPTION, PAYLOAD DATA > MTU

Procedure:

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	SEND	CS OS Console	Send a User Data greater than MTU size	`scp uas-user@ua:validation-logs/TP-CM-005B.txt validation-logs/TP-CM-005B-2.txt`
2	IR-09b	VERIFY	CS Main Sniffer	User Data > MTU is segmented	Verify via the traffic sniffer log that User Data was segmented


cs.main.sniffer.2023.09.08-09.54.40.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port==51102
Frame (1112 bytes)
Decrypted DTLS (1011 bytes)

```
No.   Time            Source              Destination         Protocol  Length Info
46789 2508.036104135  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   712 Application Data
46790 2508.079719203  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   193 Application Data
46791 2508.149179187  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   216 Application Data
46792 2508.150677091  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   300 Application Data
46795 2508.456275062  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   221 Application Data
46799 2508.526878090  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2  1112 Application Data
46800 2508.569391994  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   188 Application Data
46813 2508.947524638  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   232 Application Data
46814 2508.948963159  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   188 Application Data
46816 2508.949925179  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   324 Application Data
46821 2509.315421185  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   260 Application Data
46822 2509.316606526  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data
46825 2509.693582565  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   248 Application Data
46826 2509.694708235  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data
46839 2510.034186646  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   196 Application Data
```

```
Frame 46799: 1112 bytes on wire (8896 bits), 1112 bytes captured (8896
    Section number: 1
  > Interface id: 2 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  8, 2023 10:36:29.496090588 Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694187389.496090588 seconds
    [Time delta from previous captured frame: -0.042540207 seconds]
    [Time delta from previous displayed frame: 0.070603028 seconds]
    [Time since reference or first frame: 2508.526878090 seconds]
    Frame Number: 46799
    Frame Length: 1112 bytes (8896 bits)
    Capture Length: 1112 bytes (8896 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde
> User Datagram Protocol, Src Port: 54926, Dst Port: 51102
v Datagram Transport Layer Security
  > DTLSv1.2 Record Layer: Application Data Protocol: Application Data
v Data (1011 bytes)
    Data: 05f303d301000002000000000d0000007f000000f00300000000000000008eff717
    [Length: 1011]
```

```
0000  45 00 04 58 6a 72 40 00  ff 29 f8 df 0a 14
0010  0a 14 00 02 60 02 2a c6  04 1c 11 40 fd 00
0020  dd e0 00 00 00 00 00 00  00 00 00 0a fd 00
0030  dd e0 00 00 00 00 00 00  00 00 00 0f d6 8e
0040  04 1c 6b 23 17 fe fd 00  01 00 00 00 00 01
0050  07 05 f3 03 d3 01 00 00  02 00 00 00 0d 00
0060  7f 00 00 00 f0 03 00 00  00 00 00 00 00 8e
0070  7f 00 00 00 45 00 03 d0  90 98 40 00 40 06
0080  0a 64 00 01 0a 64 00 02  00 16 c1 9e 43 13
0090  4d ac 86 b9 80 18 01 f5  1f 7f 00 00 01 01
00a0  16 46 43 be 8b 09 75 53  49 9f 60 04 a6 46
00b0  30 0b 33 c6 f2 01 00 ac  1b dc 8f 38 de 23
00c0  03 c5 4e 2c ba d3 05 cd  fa fd b0 13 23 48
00d0  80 0b 4e 5b 03 eb f4 96  05 80 d6 a2 4b 96
00e0  62 99 1f 5c 75 da f4 94  3f 17 1c 8d 85 b5
00f0  1f d7 aa 45 82 2d b3 a0  cb a7 cf ce 87 74
0100  d6 55 14 5a 58 a5 d6 6c  d4 46 3f ba 27 66
0110  60 46 e6 6d d2 7a aa 8e  a3 d7 68 35 8f 31
0120  b3 12 e7 d6 c1 4c 0f ba  05 38 c1 32 1e e9
0130  13 c5 85 0f d9 cd 57 6c  dc 41 de e9 ec 35
0140  9e 48 42 58 4a 93 87 ef  60 36 42 15 9c 54
0150  d0 52 6f 10 ab 2d 21 cb  eb 9e be 71 da f5
0160  93 0c 36 76 b2 59 b5 11  e2 b0 e7 fe 22 d6
0170  88 60 c9 db 69 a5 e8 56  a8 1f 85 73 a6 a1
0180  bf e4 cd 28 75 42 bf 96  b1 66 34 d0 5d 62
0190  53 e5 81 c7 79 f4 ae bf  f2 5b 9e f7 d7 77
01a0  f1 77 fb 1c 27 93 6b 3d  90 2d b6 f8 94 f7
01b0  34 c8 e4 fd b4 b8 7e d9  e3 ec 09 24 59 b8
01c0  e9 26 57 cc 6b 25 d3 7f  07 cb 66 b5 50 a9
```

CS Sniffer shows messages of max length 1112 for the duration of the file transfer.

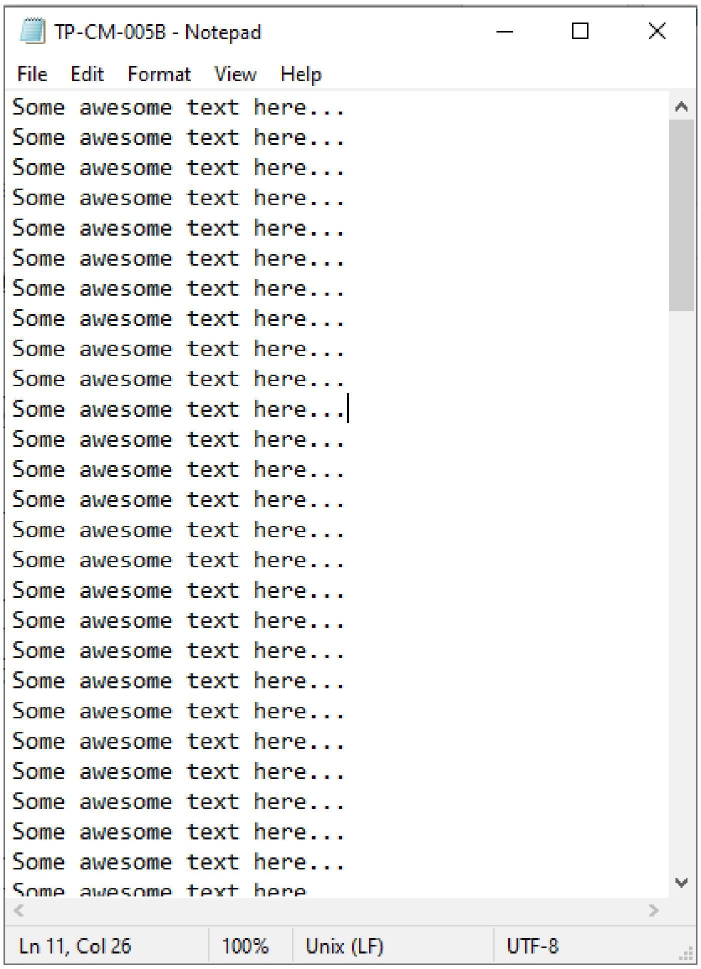
The payload data shows encrypted because it was transferred using Secure Copy Protocol (SCP), even though the link was not encrypted.

Post-test Log Analysis

STEP	REQ	Action	Component	Description	Procedure
3	SER-02	VERIFY	UA and CS Content Directory	User Data received matches User Data sent which indicates the message was accepted as authentic.	Compare the received User Data file with the source User Data file on the UA to show that the sent and received contents are the same

STEP	REQ	Action	Component	Description	Procedure

Text file sent and received matches.



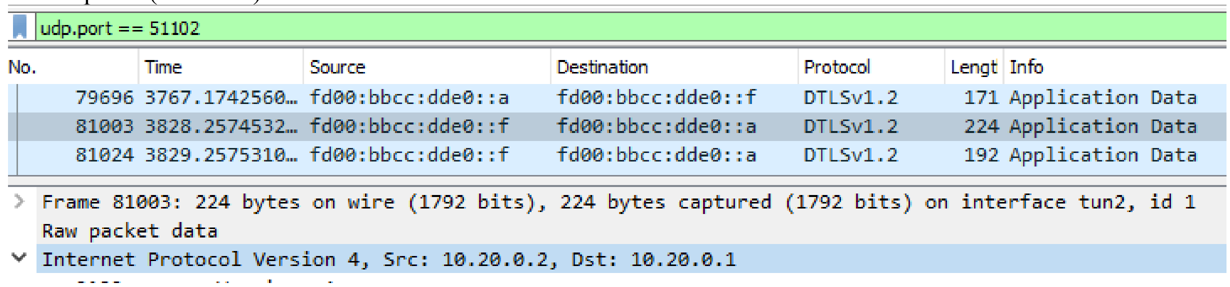
```
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here...
Some awesome text here
```

A.1.6 TP_CM_006 – User Data and Control Message Exchange with interruption < TET

STEP	REQ	Action	Component	Description	Procedure
1		VERIFY	CS Main Sniffer	Control Messages are sent and User Data messages are received over the active link	Verify via the traffic sniffer log that: a) Verify that the User Data messages are only received via the link supporting the active connection b) Verify that Control Messages are sent to the UA via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure

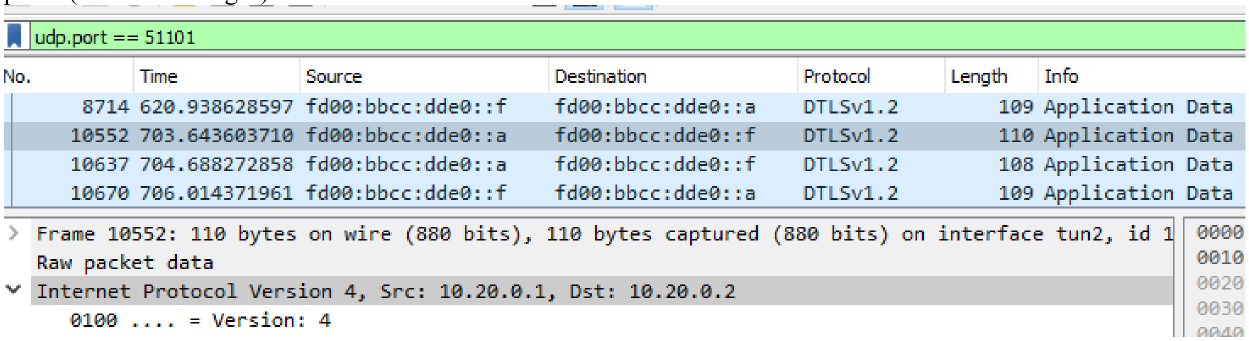
Source address 10.20.0.2 is the CS on LTE; destination address of 10.20.0.1 is the UA on LTE. Udp.port 51102 is user plane (user data)



udp.port == 51102

```
No.    Time            Source             Destination        Protocol   Lengt Info
 79696 3767.1742560… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    171 Application Data
 81003 3828.2574532… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    224 Application Data
 81024 3829.2575310… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    192 Application Data

> Frame 81003: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
```

Source address 10.20.0.2 is CS on LTE; destination address 10.20.0.1 is UA on LTE. Udp port 51101 is control plane (control messages).



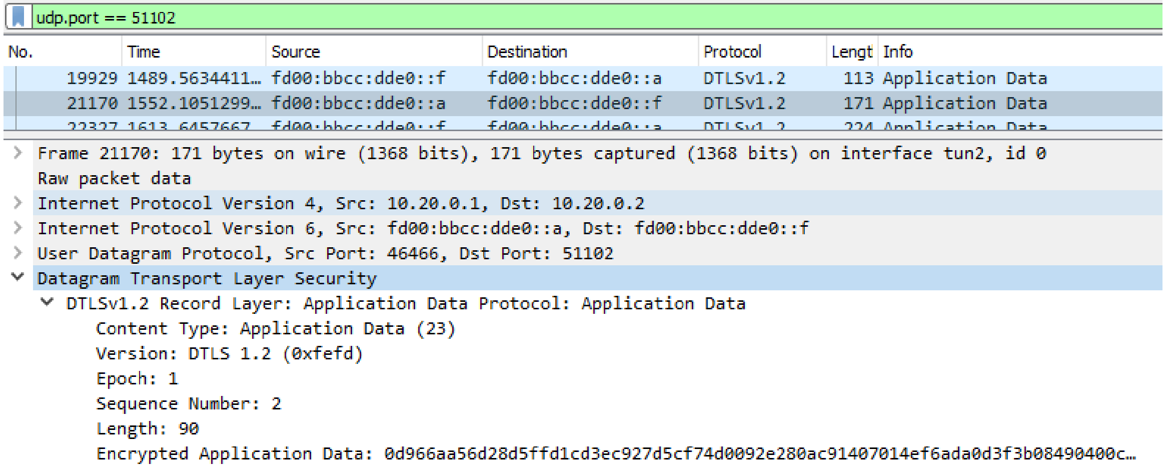
udp.port == 51101

```
No.    Time          Source             Destination        Protocol   Length Info
  8714 620.938628597 fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      109 Application Data
 10552 703.643603710 fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      110 Application Data
 10637 704.688272858 fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2      108 Application Data
 10670 706.014371961 fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2      109 Application Data

> Frame 10552: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface tun2, id 1   0000
  Raw packet data                                                                                    0010
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2                                        0020
    0100 .... = Version: 4                                                                           0030
```

2		VERIFY	UA Main Sniffer	Control Messages are sent and User Data messages are received over the active link	Verify via the traffic sniffer log that: a) Verify that the User Data messages are only received via the link supporting the active connection b) Verify that the Control Data Messages are received by the UA via the link supporting the active Connection

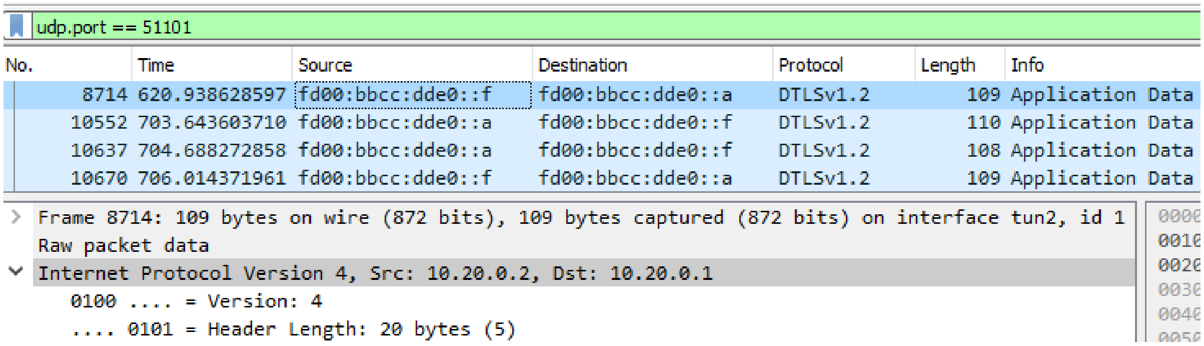
STEP	REQ	Action	Component	Description	Procedure

Source address 10.20.0.1 is the UA on LTE; destination address 10.20.0.2 is the CS on LTE; Udp port 51102 is user plane (user data).



```
udp.port == 51102

No.     Time              Source              Destination         Protocol   Lengt Info
  19929 1489.5634411…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   113 Application Data
  21170 1552.1051299…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   171 Application Data
  22327 1613.6457667      fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   224 Application Data

> Frame 21170: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface tun2, id 0
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 46466, Dst Port: 51102
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
        Content Type: Application Data (23)
        Version: DTLS 1.2 (0xfefd)
        Epoch: 1
        Sequence Number: 2
        Length: 90
        Encrypted Application Data: 0d966aa56d28d5ffd1cd3ec927d5cf74d0092e280ac91407014ef6ada0d3f3b08490400c…
```

Source address 10.20.0.2 is CS on LTE; destination address of 10.20.0.1 is UA on LTE. Udp port 51101 is control plane (control messages)



```
udp.port == 51101

No.    Time            Source              Destination         Protocol   Length Info
  8714 620.938628597   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      109 Application Data
 10552 703.643603710   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      110 Application Data
 10637 704.688272858   fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      108 Application Data
 10670 706.014371961   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      109 Application Data

> Frame 8714: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface tun2, id 1
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
```

3	IR-10	INVOKE	CS OS Console	Interrupt the Secure Connection between UA & CS DTSR for a time < TET	`disable_link <ID>`
					`enable_link <ID>`

4	IR-10	VERIFY	UA or CS LMSF Console	CS status shows:
				…secure session is established
				…the same link is providing the connection after the interruption
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

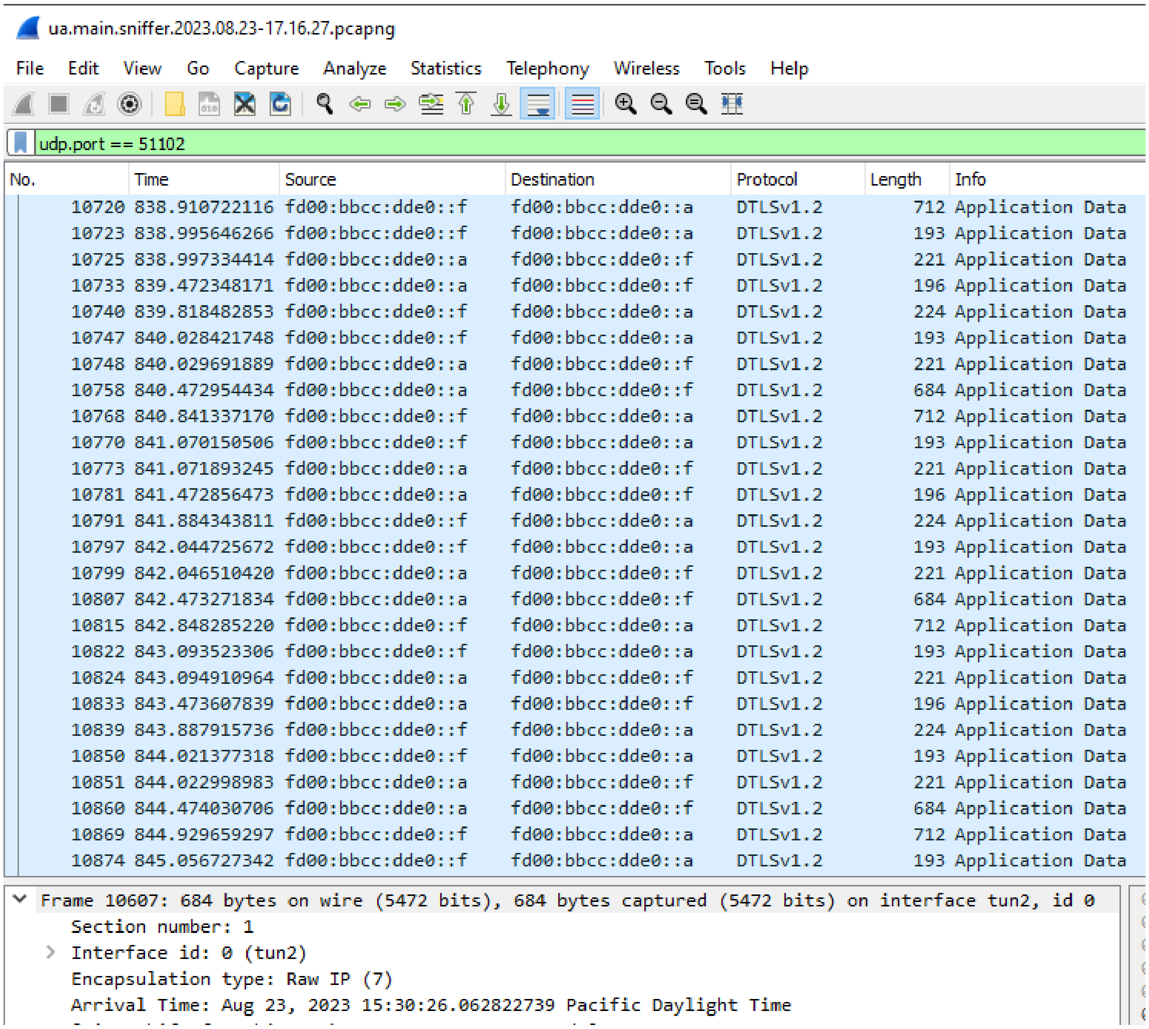
```
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

Post-test Log Analysis

STEP	REQ	Action	Component	Description	Procedure
5	IR-10	VERIFY	UA and CS DTSR Inspect Log	Examine result of interruption < TET	Verify via the inspect logs that: a) the UA DTSR did not indicate an interruption > TET b) all User Data messages sent before and after the interruption are received c) all Control Messages sent are received

STEP REQ Action Component Description Procedure

The UA Main Sniffer shows the user data messages are sent/received for the entirety of the interruption time.



ua.main.sniffer.2023.08.23-17.16.27.pcapng

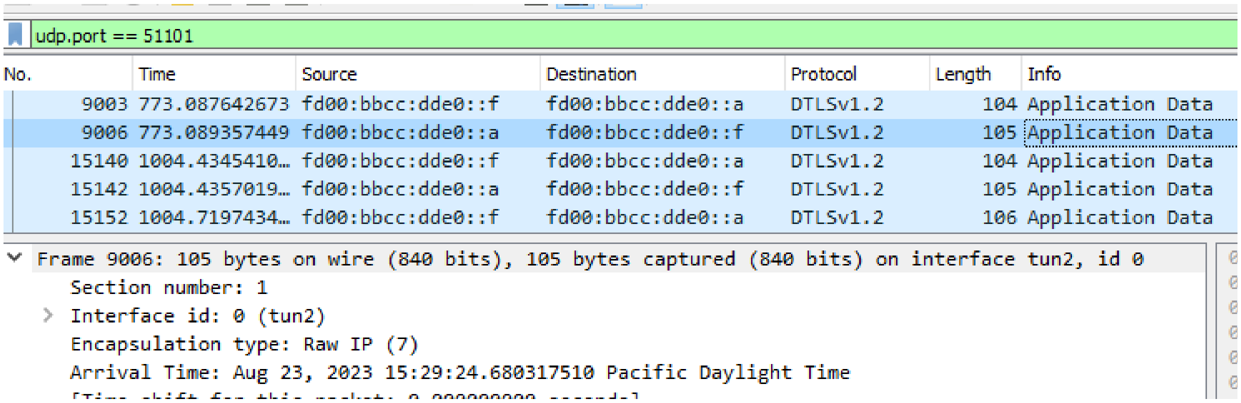
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 51102

```
No.    Time          Source            Destination       Protocol  Length Info
 10720 838.910722116 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     712 Application Data
 10723 838.995646266 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10725 838.997334414 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10733 839.472348171 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     196 Application Data
 10740 839.818482853 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     224 Application Data
 10747 840.028421748 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10748 840.029691889 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10758 840.472954434 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     684 Application Data
 10768 840.841337170 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     712 Application Data
 10770 841.070150506 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10773 841.071893245 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10781 841.472856473 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     196 Application Data
 10791 841.884343811 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     224 Application Data
 10797 842.044725672 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10799 842.046510420 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10807 842.473271834 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     684 Application Data
 10815 842.848285220 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     712 Application Data
 10822 843.093523306 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10824 843.094910964 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10833 843.473607839 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     196 Application Data
 10839 843.887915736 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     224 Application Data
 10850 844.021377318 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
 10851 844.022998983 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     221 Application Data
 10860 844.474030706 fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     684 Application Data
 10869 844.929659297 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     712 Application Data
 10874 845.056727342 fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     193 Application Data
```

```
Frame 10607: 684 bytes on wire (5472 bits), 684 bytes captured (5472 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 23, 2023 15:30:26.062822739 Pacific Daylight Time
```

Control plane messages continue for the length of the interruption.



udp.port == 51101

```
No.    Time           Source            Destination       Protocol  Length Info
  9003 773.087642673  fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     104 Application Data
  9006 773.089357449  fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     105 Application Data
 15140 1004.4345410…  fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     104 Application Data
 15142 1004.4357019…  fd00:bbcc:dde0::a fd00:bbcc:dde0::f DTLSv1.2     105 Application Data
 15152 1004.7197434…  fd00:bbcc:dde0::f fd00:bbcc:dde0::a DTLSv1.2     106 Application Data
```

```
Frame 9006: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 23, 2023 15:29:24.680317510 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
```

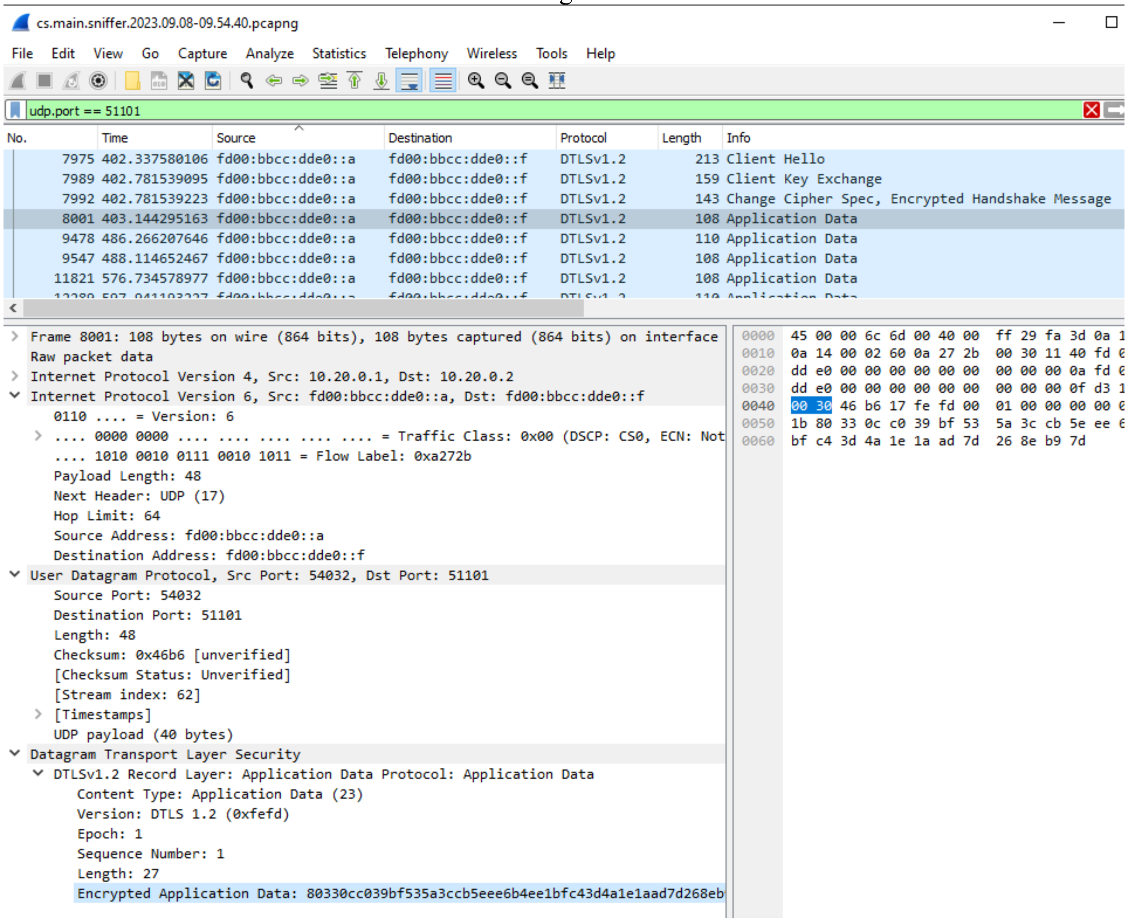
STEP	REQ	Action	Component	Description	Procedure
6	IR-10	VERIFY	CS DTSR Inspect logs	Examine result of interruption < TET	Verify via the inspect logs that: a) the CS DTSR did not indicate an interruption > TET b) all User Data and Control Messages are sent despite the interruption c) all User Data and Control Messages are received

No evidence of interruption in CS DTSR log for the entirety of the interruption.

Performance data shows all UA downlinks are sent for the duration of the interruption, and all CS uplinks are sent for the duration of the interruption.

A.1.7 TP_CM_007 – Control Message Exchanges with Encryption

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	OBSERVE	CS DTSR Inspect Log	Status Reports are being sent	View the periodic Status Reports from the UA
2	IR-09b	VERIFY	CS Main Sniffer	Control Message < MTU does not require segmentation	Verify via the traffic sniffer log that segmentation does not occur



udp.port == 51101

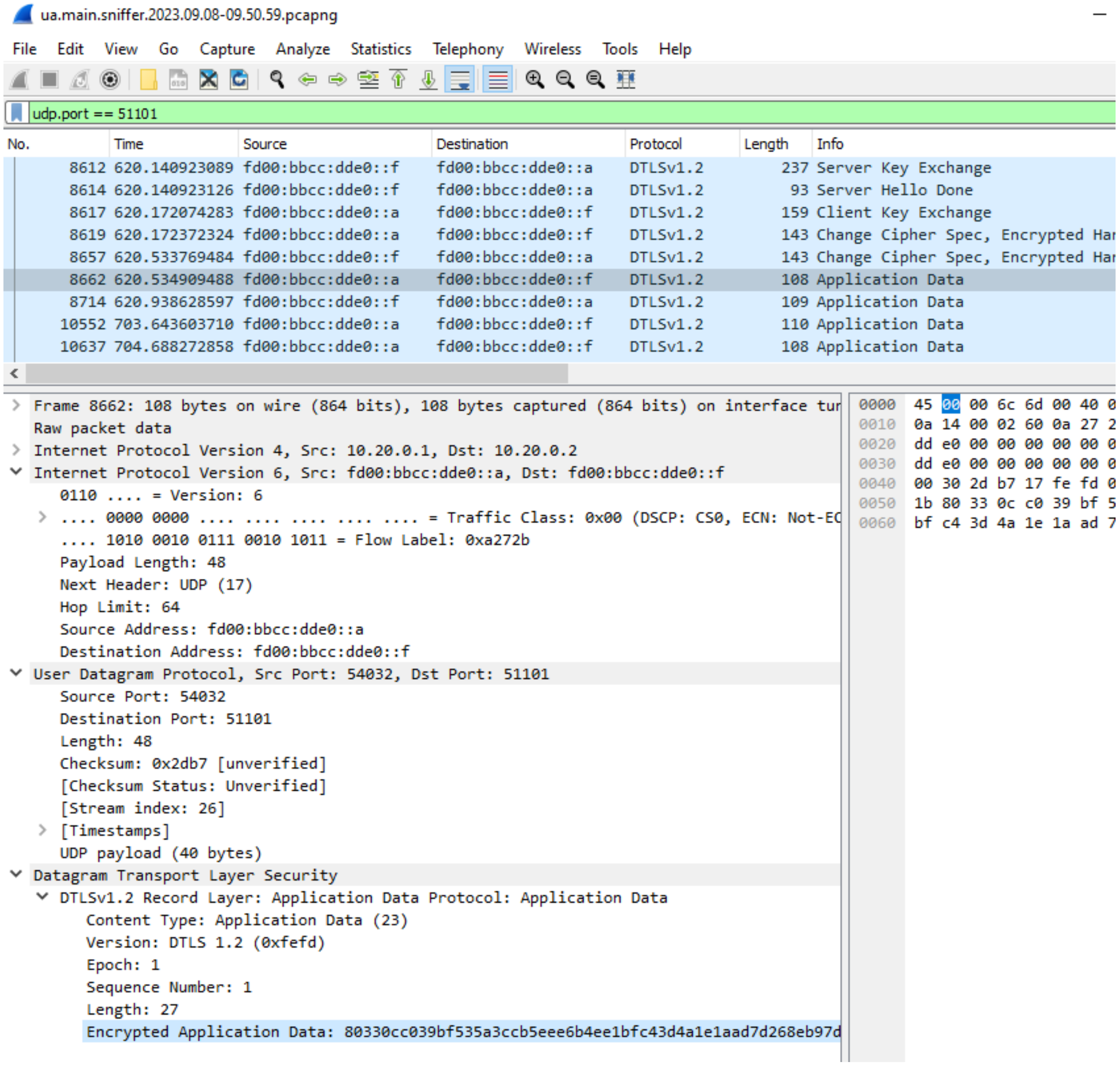
```
No.    Time          Source               Destination          Protocol   Length Info
  7975 402.337580106 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      213 Client Hello
  7989 402.781539095 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      159 Client Key Exchange
  7992 402.781539223 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      143 Change Cipher Spec, Encrypted Handshake Message
  8001 403.144295163 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      108 Application Data
  9478 486.266207646 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      110 Application Data
  9547 488.114652467 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      108 Application Data
 11821 576.734578977 fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      108 Application Data
```

```
> Frame 8001: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not
    .... 1010 0010 0111 0010 1011 = Flow Label: 0xa272b
    Payload Length: 48
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
v User Datagram Protocol, Src Port: 54032, Dst Port: 51101
    Source Port: 54032
    Destination Port: 51101
    Length: 48
    Checksum: 0x46b6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 62]
  > [Timestamps]
    UDP payload (40 bytes)
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 1
      Length: 27
      Encrypted Application Data: 80330cc039bf535a3ccb5eee6b4ee1bfc43d4a1e1aad7d268eb
```

```
0000  45 00 00 6c 6d 00 40 00  ff 29 fa 3d 0a 1
0010  0a 14 00 02 60 0a 27 2b  00 30 11 40 fd 0
0020  dd e0 00 00 00 00 00 00  00 00 00 0a fd 0
0030  dd e0 00 00 00 00 00 00  00 00 00 0f d3 1
0040  00 30 46 b6 17 fe fd 00  01 00 00 00 00 0
0050  1b 80 33 0c c0 39 bf 53  5a 3c cb 5e ee 6
0060  bf c4 3d 4a 1e 1a ad 7d  26 8e b9 7d
```

CS Main sniffer filtered on the control plane traffic (udp port 51101) shows messages are not segmented.

STEP	REQ	Action	Component	Description	Procedure
3	SER-09 SER-11	VERIFY	UA and CS Main Sniffers	Control Message received matches Control Message sent which indicates the message was accepted as authentic.	Compare the two sniffer logs to verify the received Control Message has the same contents as the one that was sent



```
udp.port == 51101

No.     Time          Source              Destination         Protocol   Length Info
   8612 620.140923089 fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   237 Server Key Exchange
   8614 620.140923126 fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    93 Server Hello Done
   8617 620.172074283 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   159 Client Key Exchange
   8619 620.172372324 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   143 Change Cipher Spec, Encrypted Har
   8657 620.533769484 fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   143 Change Cipher Spec, Encrypted Har
   8662 620.534909488 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   108 Application Data
   8714 620.938628597 fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   109 Application Data
  10552 703.643603710 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   110 Application Data
  10637 704.688272858 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   108 Application Data
```

```
> Frame 8662: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface tur
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-EC
    .... 1010 0010 0111 0010 1011 = Flow Label: 0xa272b
    Payload Length: 48
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
v User Datagram Protocol, Src Port: 54032, Dst Port: 51101
    Source Port: 54032
    Destination Port: 51101
    Length: 48
    Checksum: 0x2db7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 26]
  > [Timestamps]
    UDP payload (40 bytes)
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 1
      Length: 27
      Encrypted Application Data: 80330cc039bf535a3ccb5eee6b4ee1bfc43d4a1e1aad7d268eb97d
```

```
0000  45 00 00 6c 6d 00 40 0
0010  0a 14 00 02 60 0a 27 2
0020  dd e0 00 00 00 00 00 0
0030  dd e0 00 00 00 00 00 0
0040  00 30 2d b7 17 fe fd 0
0050  1b 80 33 0c c0 39 bf 5
0060  bf c4 3d 4a 1e 1a ad 7
```

Identical message is found in the UA Main sniffer.

4	SER-11	VERIFY	UA Main Sniffer	Control Message content cannot be discerned from the message in-transit (i.e., encrypted)	Verify via the traffic sniffer log that secure Control Message is transmitted

UA Main sniffer log shows application data is encrypted.

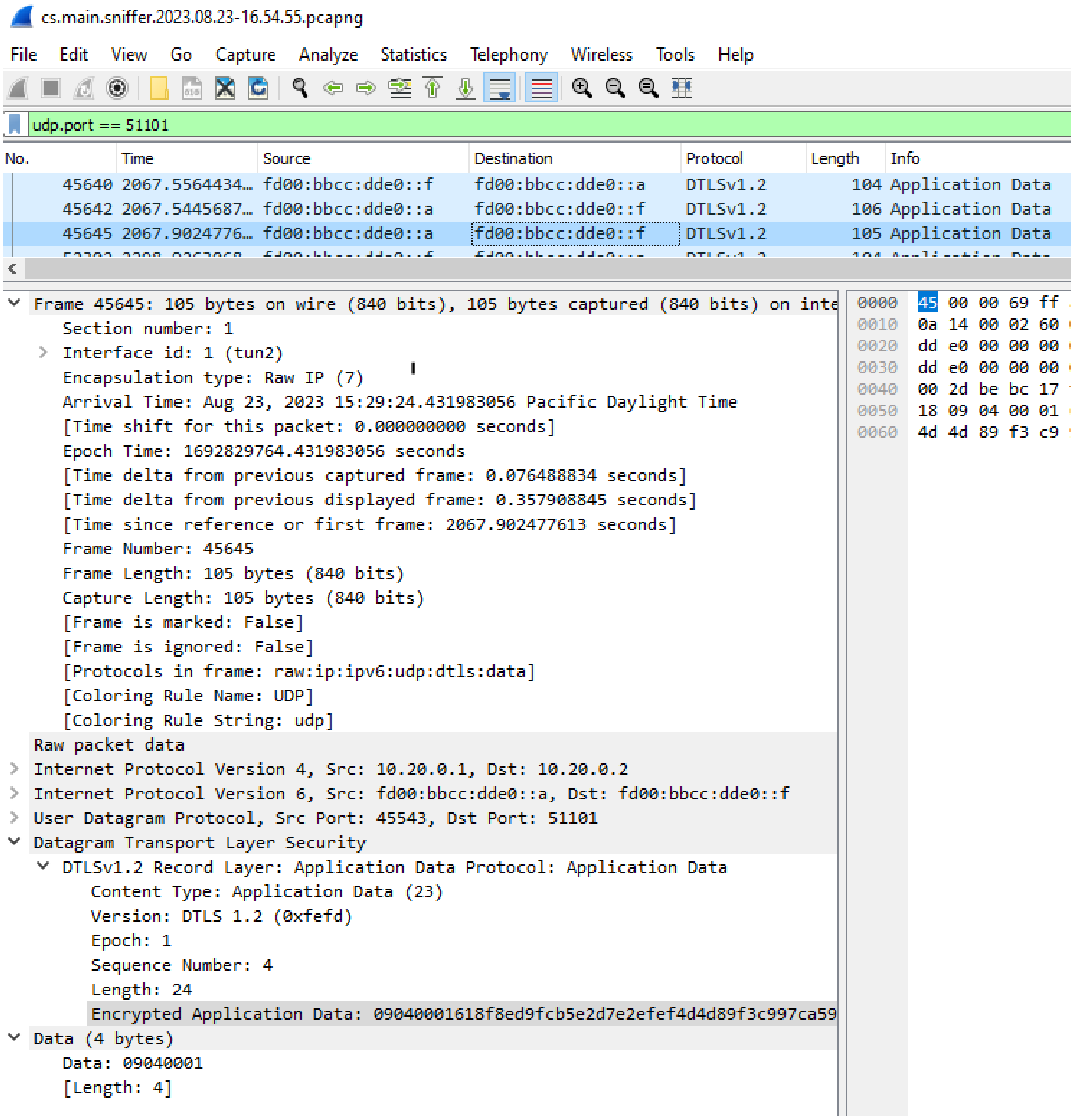
5	SER-11	VERIFY	CS Main Sniffer	Control Message content cannot be discerned from the message in-transit (i.e., encrypted)	Verify via the traffic sniffer log that the content of secure Control Message transmitted does not reveal content at the monitoring point

CS Main sniffer log shows application data is encrypted.

A.1.8 TP_CM_008 – Control Message Exchanges without Encryption

STEP	REQ	Action	Component	Description	Procedure
1	IR-09b	OBSERVE	CS DTSR Inspect Log	Status Reports are being sent	View the periodic Status Reports from the UA
2	IR-09b IR-02	VERIFY	CS Main Sniffer	Control Message < MTU does not require segmentation	Verify via the traffic sniffer log that: a) message segmentation does not occur for messages < MTU b) Control Messages include unique IP source and destination addresses that uniquely identify the UA and CS

CS Main Sniffer log shows control messages are not segmented (length is 105).
IPv6 addresses are unique. Fd00:bbcc:dde0::a is the UA DSTR; fd00:bbcc:dde0::f is the CS DTSR.



cs.main.sniffer.2023.08.23-16.54.55.pcapng

udp.port == 51101

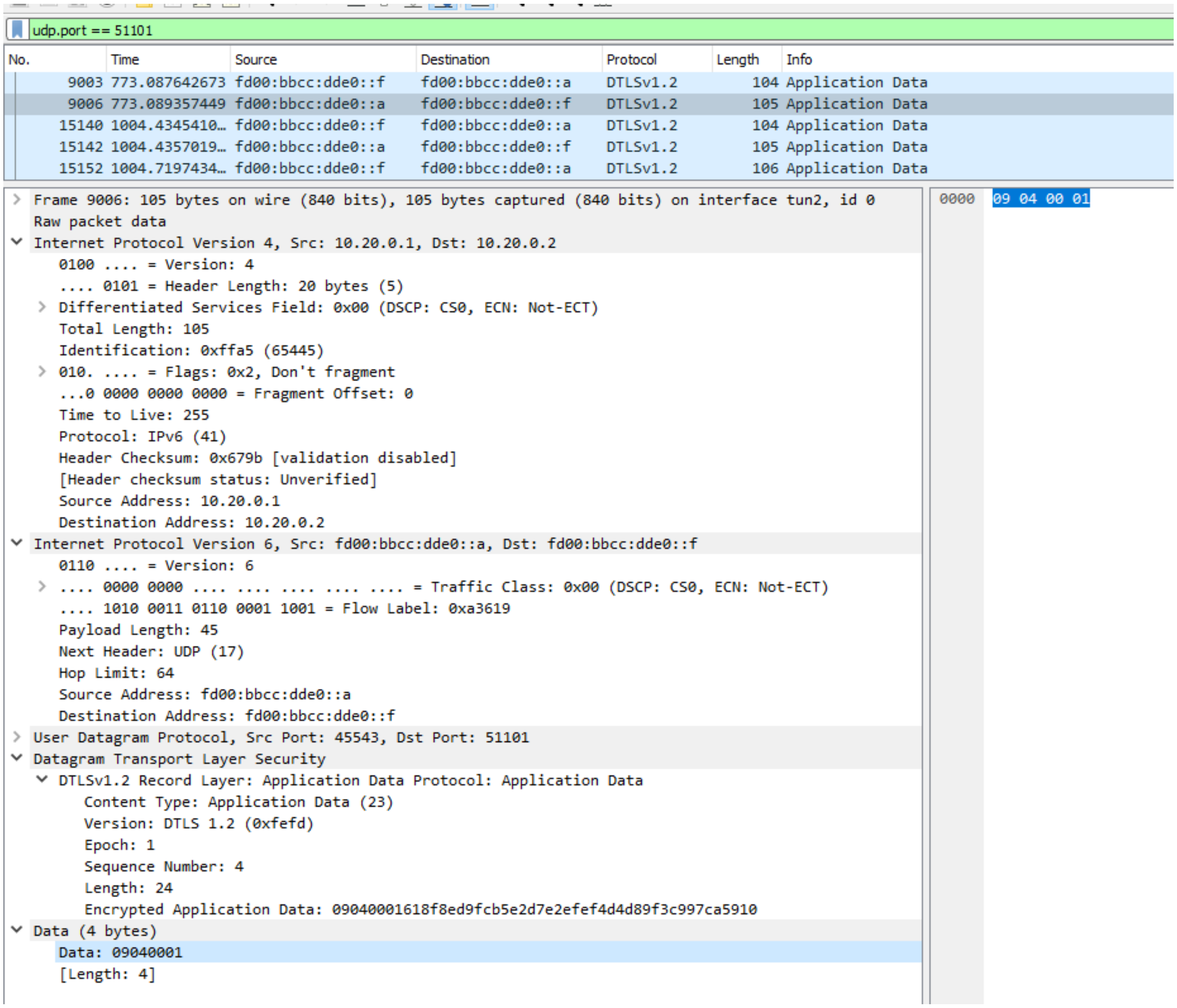
```
No.     Time              Source              Destination         Protocol   Length Info
  45640 2067.5564434…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2     104 Application Data
  45642 2067.5445687…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2     106 Application Data
  45645 2067.9024776…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2     105 Application Data
```

```
Frame 45645: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on inte
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 23, 2023 15:29:24.431983056 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692829764.431983056 seconds
    [Time delta from previous captured frame: 0.076488834 seconds]
    [Time delta from previous displayed frame: 0.357908845 seconds]
    [Time since reference or first frame: 2067.902477613 seconds]
    Frame Number: 45645
    Frame Length: 105 bytes (840 bits)
    Capture Length: 105 bytes (840 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
User Datagram Protocol, Src Port: 45543, Dst Port: 51101
Datagram Transport Layer Security
  DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 4
      Length: 24
      Encrypted Application Data: 09040001618f8ed9fcb5e2d7e2efef4d4d89f3c997ca59
Data (4 bytes)
    Data: 09040001
    [Length: 4]
```

```
0000  45 00 00 69 ff
0010  0a 14 00 02 60
0020  dd e0 00 00 00
0030  dd e0 00 00 00
0040  00 2d be bc 17
0050  18 09 04 00 01
0060  4d 4d 89 f3 c9
```

STEP	REQ	Action	Component	Description	Procedure
3	SER-09	VERIFY	CS and UA Main Sniffers	Control Message received matches Control Message sent which indicates the message was accepted as authentic.	Verify via the traffic sniffer logs that: a) the received Control Message has the same contents as the one that was sent b) the secure Control Message contains an authentication tag and the tag length is at least 64 bits

a) UA Main sniffer shows the exact same control message, where application data is 0904001.



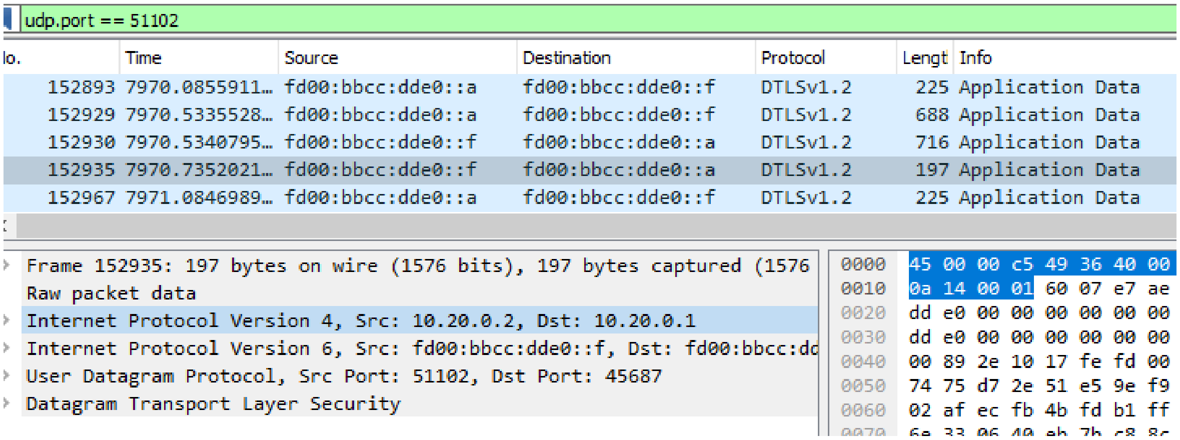
```
udp.port == 51101

No.        Time           Source              Destination         Protocol   Length  Info
     9003 773.087642673 fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      104 Application Data
     9006 773.089357449 fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      105 Application Data
    15140 1004.4345410… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      104 Application Data
    15142 1004.4357019… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      105 Application Data
    15152 1004.7197434… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      106 Application Data

> Frame 9006: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface tun2, id 0
  Raw packet data
v Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 105
    Identification: 0xffa5 (65445)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: IPv6 (41)
    Header Checksum: 0x679b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.20.0.1
    Destination Address: 10.20.0.2
v Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0110 0001 1001 = Flow Label: 0xa3619
    Payload Length: 45
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: fd00:bbcc:dde0::a
    Destination Address: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 45543, Dst Port: 51101
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 4
      Length: 24
      Encrypted Application Data: 09040001618f8ed9fcb5e2d7e2efef4d4d89f3c997ca5910
v Data (4 bytes)
    Data: 09040001
    [Length: 4]

0000  09 04 00 01
```

b) Above sniffer log shows the application data payload is 4 bytes; the remaining 20 bytes is the tag. The registered NULL cipher suite invokes the user of HMAC with the SHA-1 hash algorithm which produces a non-truncated 20 byte (160 bit) authentication tag.

A.1.9 TP_CM_009 – Link Switchover < TET

Example from Flight 2; LTE to SATCOM on Aug 24th at 1:07.

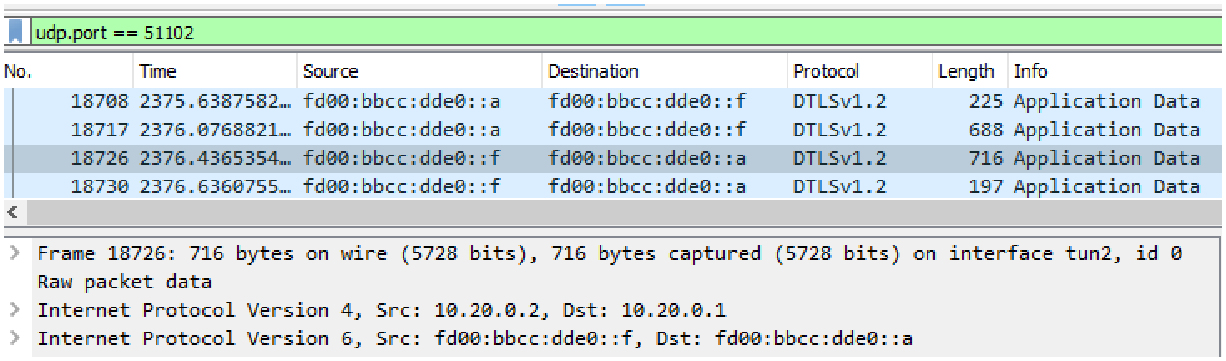
STEP	REQ	Action	Component	Description	Procedure
1	IR-04	VERIFY	CS Main Sniffer	Verify that User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent by the CS via the link supporting the active Connection



```
udp.port == 51102

No.   Time               Source               Destination          Protocol  Lengt Info
 152893 7970.0855911… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   225 Application Data
 152929 7970.5335528… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   688 Application Data
 152930 7970.5340795… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   716 Application Data
 152935 7970.7352021… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   197 Application Data
 152967 7971.0846989… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   225 Application Data

> Frame 152935: 197 bytes on wire (1576 bits), 197 bytes captured (1576    0000  45 00 00 c5 49 36 40 00
  Raw packet data                                                          0010  0a 14 00 01 60 07 e7 ae
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1              0020  dd e0 00 00 00 00 00 00
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dd   0030  dd e0 00 00 00 00 00 00
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687                 0040  00 89 2e 10 17 fe fd 00
> Datagram Transport Layer Security                                        0050  74 75 d7 2e 51 e5 9e f9
                                                                           0060  02 af ec fb 4b fd b1 ff
```

Messages from the CS are sent from 10.20.0.2, which is LTE.

STEP	REQ	Action	Component	Description	Procedure
2	IR-04	VERIFY	UA Main Sniffer	Verify that User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received by the UA via the link supporting the active Connection



```
udp.port == 51102

No.     Time               Source               Destination          Protocol   Length Info
   18708 2375.6387582… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      225 Application Data
   18717 2376.0768821… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2      688 Application Data
   18726 2376.4365354… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      716 Application Data
   18730 2376.6360755… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2      197 Application Data

> Frame 18726: 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface tun2, id 0
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
```

Messages received by the UA have destination 10.20.0.1, which is LTE.

STEP	REQ	Action	Component	Description	Procedure

3	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf`
					`lmsf> status`

4	IR-08	OBSERVE	UA LMSF Console	View the status of all available links	`cs-sh lmsf`
					`lmsf> status`

5	IR-05	SEND	CS LMSF Console	Issue Switchover command for the desired alternate link	`lmsf`
					`lmsf> switch 1`

```
2023-08-24 18:07:56.279090 GMT INFO     ControlOut.cpp:294
Initiating switchover from 2 to 1
```

STEP	REQ	Action	Component	Description	Procedure
6	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.
7	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.

STEP	REQ	Action	Component	Description	Procedure

8	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				… which link is providing the connection
				…that the secure connection is maintained following the interruption
				…the UA DTSR did not indicate an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User: Y/1 | Control: Y/1`
					No indication that the interruption was greater than TET

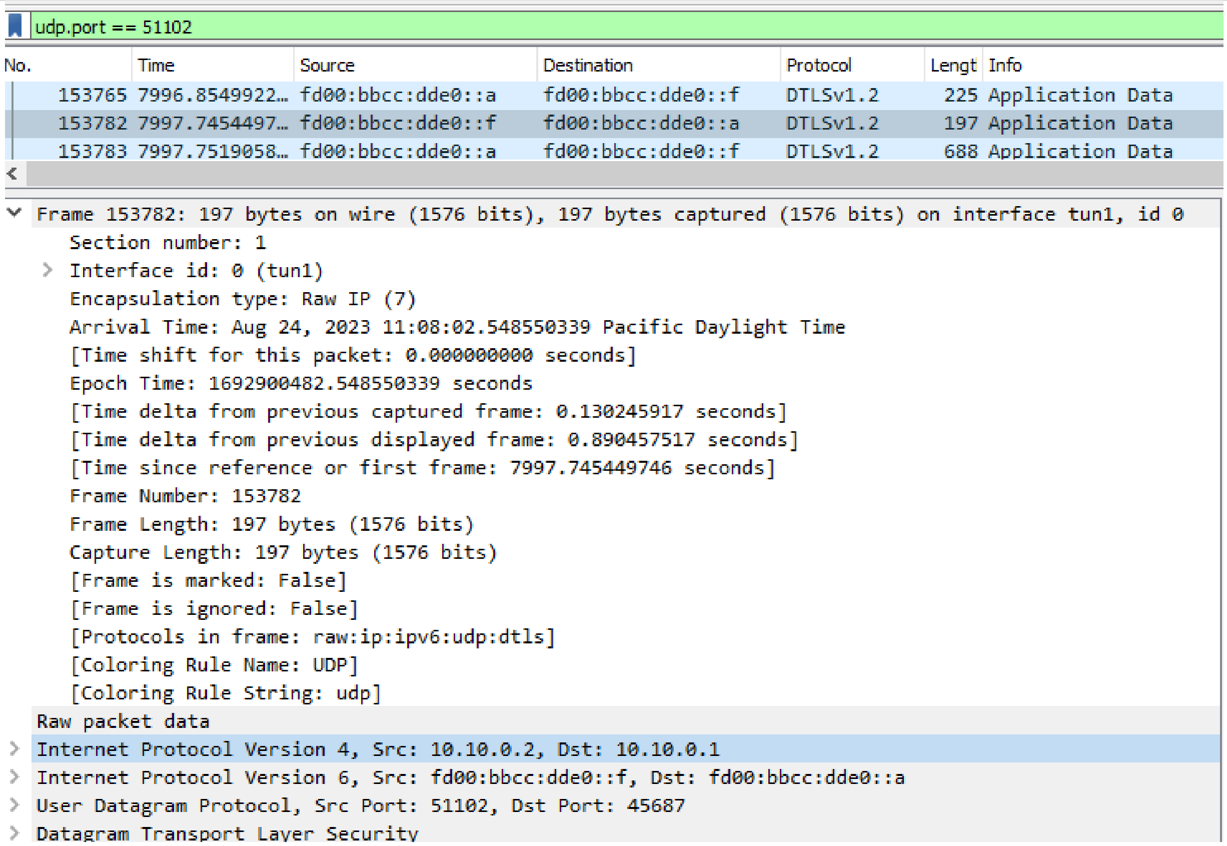
```
2023-08-24 18:08:08.827965 GMT INFO Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

9	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				… which link is providing the connection
				…that the secure connection is maintained following the interruption
				…the CS DTSR did not indicate an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User: Y/1| Control: Y/1`
					No indication that the interruption was greater than TET

```
2023-08-24 18:08:17.860622 GMT INFO Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

10	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure

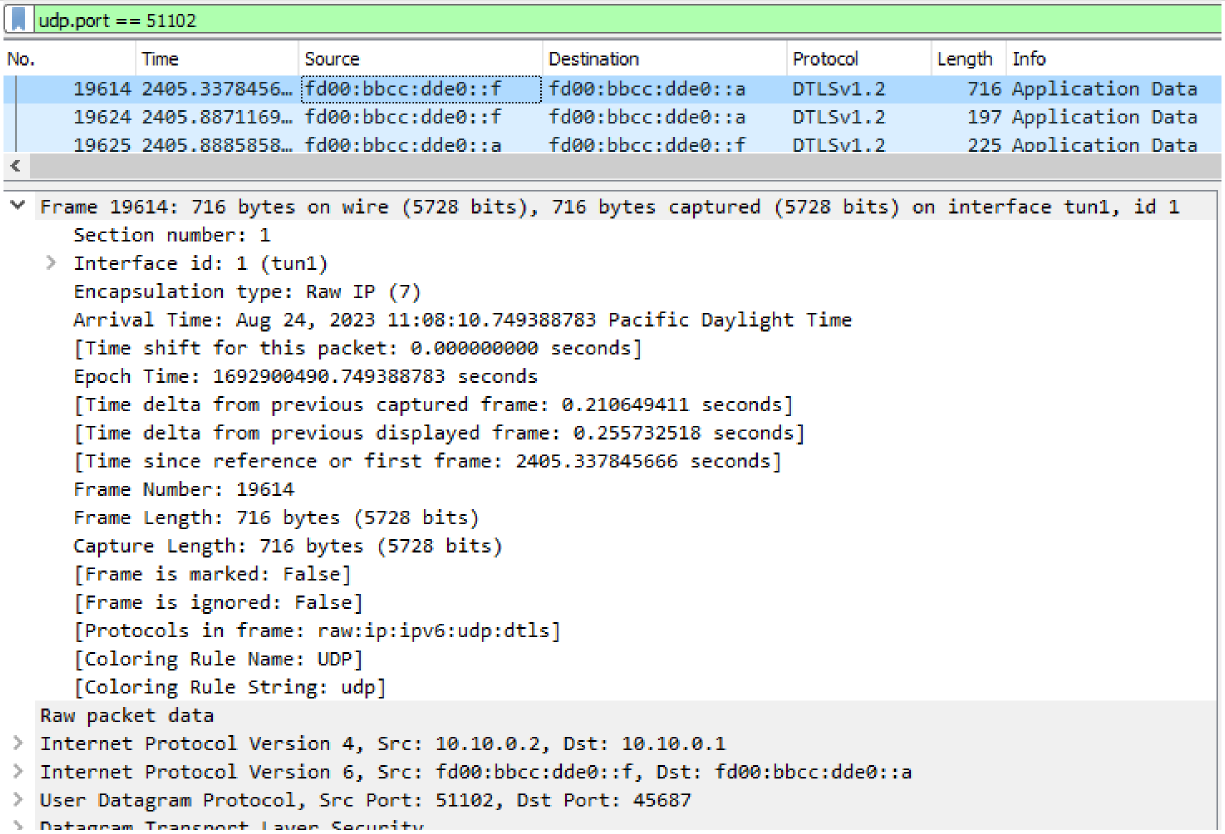


```
udp.port == 51102

No.     Time             Source              Destination         Protocol  Lengt Info
153765 7996.8549922… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    225 Application Data
153782 7997.7454497… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    197 Application Data
153783 7997.7519058… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    688 Application Data

Frame 153782: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface tun1, id 0
   Section number: 1
 > Interface id: 0 (tun1)
   Encapsulation type: Raw IP (7)
   Arrival Time: Aug 24, 2023 11:08:02.548550339 Pacific Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1692900482.548550339 seconds
   [Time delta from previous captured frame: 0.130245917 seconds]
   [Time delta from previous displayed frame: 0.890457517 seconds]
   [Time since reference or first frame: 7997.745449746 seconds]
   Frame Number: 153782
   Frame Length: 197 bytes (1576 bits)
   Capture Length: 197 bytes (1576 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: raw:ip:ipv6:udp:dtls]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687
> Datagram Transport Layer Security
```

Source address is 10.10.0.2 which is the CS on SATCOM.

11	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links

STEP	REQ	Action	Component	Description	Procedure



```
udp.port == 51102

No.    Time              Source              Destination         Protocol   Length  Info
19614  2405.3378456…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   716     Application Data
19624  2405.8871169…     fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2   197     Application Data
19625  2405.8885858…     fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2   225     Application Data

Frame 19614: 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface tun1, id 1
    Section number: 1
  > Interface id: 1 (tun1)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:08:10.749388783 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692900490.749388783 seconds
    [Time delta from previous captured frame: 0.210649411 seconds]
    [Time delta from previous displayed frame: 0.255732518 seconds]
    [Time since reference or first frame: 2405.337845666 seconds]
    Frame Number: 19614
    Frame Length: 716 bytes (5728 bits)
    Capture Length: 716 bytes (5728 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687
> Datagram Transport Layer Security
```

Destination address is 10.10.0.1 which is the UA on SATCOM.

12	IR-20	VERIFY	UA DTSR Live Log and UA Main Sniffer	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the traffic sniffer logs that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

```
2023-08-24 18:07:56.279071 GMT INFO     ControlOut.cpp:291
Sent "SWITCHOVER_REQUEST.REQ  5     2    1" across secure connection

Successful switchover to LinkInfo: 1|Type: Satellite
Name: Satellite01|Address: 10.10.0.1|Adapter: tun1
Peer: 10.10.0.2|Status: Link Up

Sent "CONNECT.REQ           3   " across secure connection
Received "CONNECT.REQ           3   " over secure session
Sent "CONNECT.CNF           4   Accepted" across secure connection
```

13	IR-20	VERIFY	CS DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via the live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

STEP	REQ	Action	Component	Description	Procedure

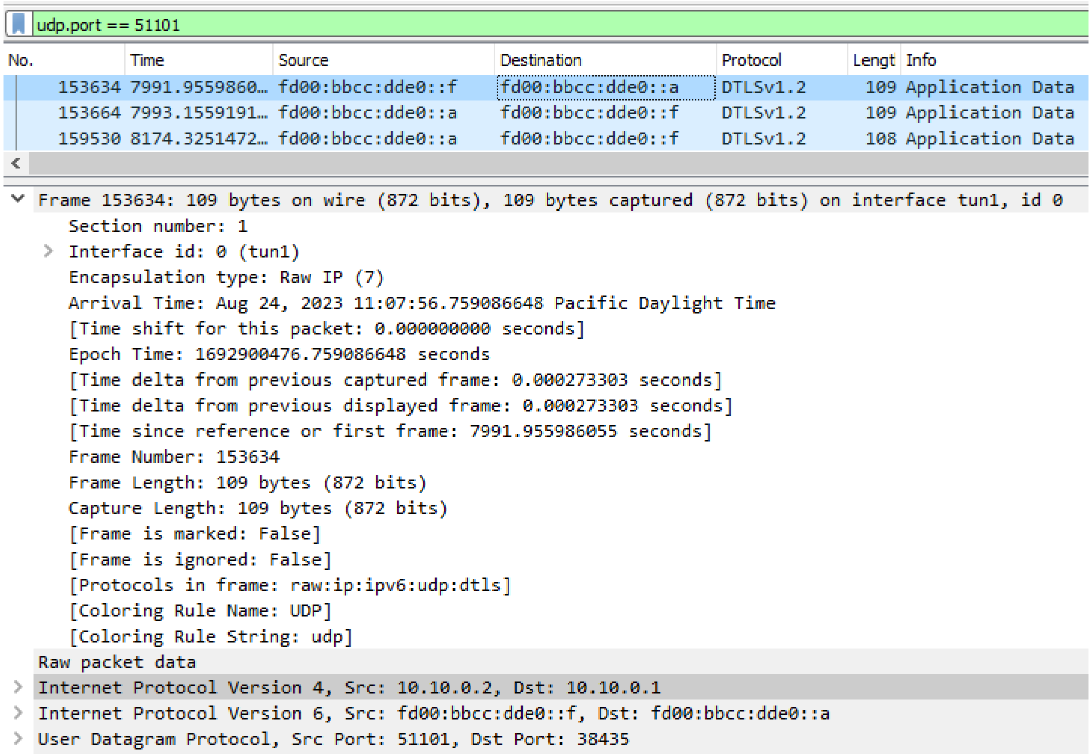
2023-08-24 18:07:56.142660 GMT INFO   ControlIn.cpp:42
Received "SWITCHOVER_REQUEST.REQ 5   2   1" over secure session

2023-08-24 18:07:56.153734 GMT INFO   LinkInfo.cpp:343
Successful switchover to LinkInfo: 1|Type: Satellite
Name: Satellite01|Address: 10.10.0.2|Adapter: tun1
Peer: 10.10.0.1|Status: Link Up

Sent "CONNECT.REQ   3   " across secure connection
Received "CONNECT.REQ   3   " over secure session
Sent "CONNECT.CNF   4   Accepted" across secure connection

14	IR-21	VERIFY	UA DTSR Live Log	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via live log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

User data looks like step 11.
Control messages are port 51101. Source address 10.10.0.2 is from the CS on SATCOM and destination address 10.10.0.1 is from the UA on SATCOM.

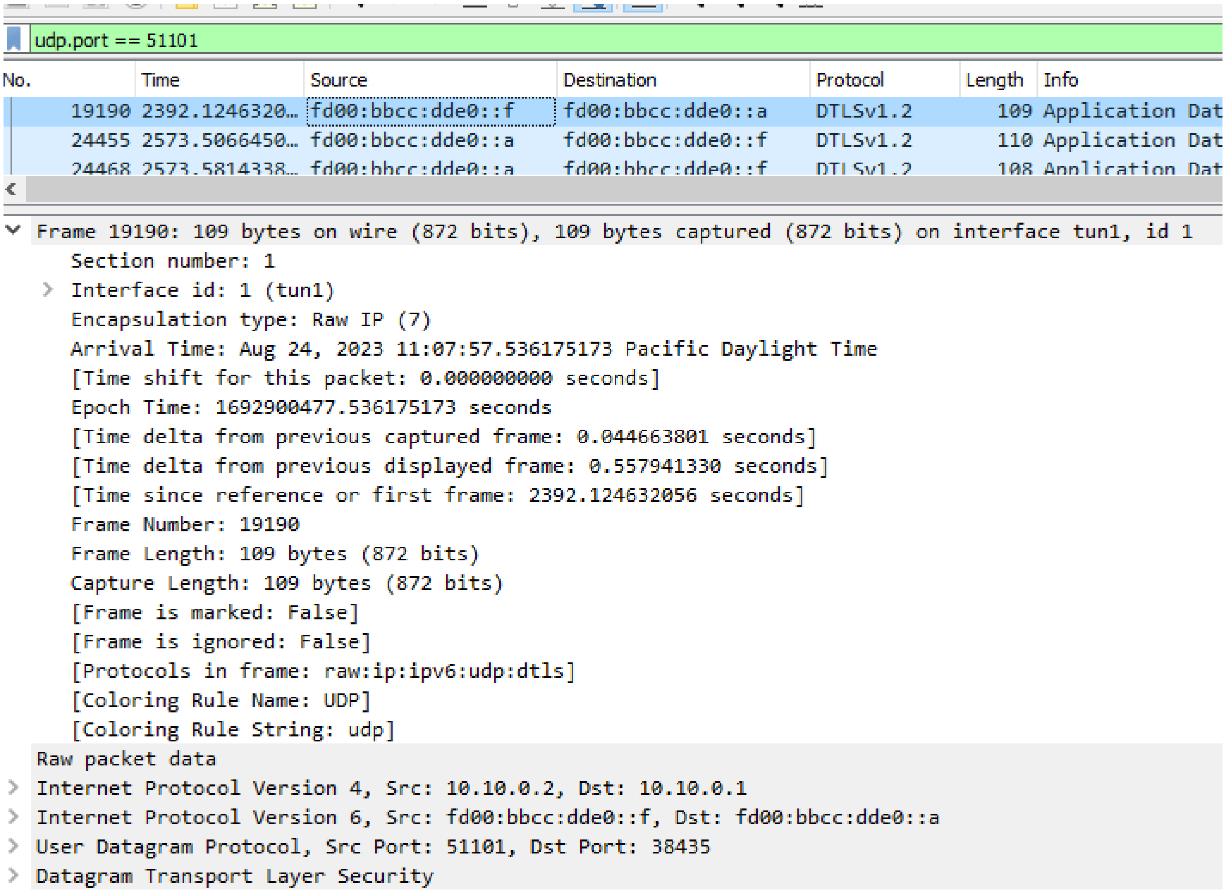


```
udp.port == 51101

No.     Time              Source             Destination        Protocol   Lengt Info
153634 7991.9559860…  fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    109 Application Data
153664 7993.1559191…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    109 Application Data
159530 8174.3251472…  fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    108 Application Data

Frame 153634: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface tun1, id 0
    Section number: 1
  > Interface id: 0 (tun1)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:07:56.759086648 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692900476.759086648 seconds
    [Time delta from previous captured frame: 0.000273303 seconds]
    [Time delta from previous displayed frame: 0.000273303 seconds]
    [Time since reference or first frame: 7991.955986055 seconds]
    Frame Number: 153634
    Frame Length: 109 bytes (872 bits)
    Capture Length: 109 bytes (872 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51101, Dst Port: 38435
```

15	IR-21	VERIFY	CS DTSR Live Log	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via live log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

STEP	REQ	Action	Component	Description	Procedure

User data looks like step 10.
Control messages are port 51101. Source address 10.10.0.2 is from the CS on SATCOM and destination address 10.10.0.1 is from the UA on SATCOM.



```
udp.port == 51101

No.     Time                Source               Destination          Protocol   Length  Info
  19190 2392.1246320…  fd00:bbcc:dde0::f    fd00:bbcc:dde0::a    DTLSv1.2      109  Application Dat
  24455 2573.5066450…  fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      110  Application Dat
  24468 2573.5814338…  fd00:bbcc:dde0::a    fd00:bbcc:dde0::f    DTLSv1.2      108  Application Dat

Frame 19190: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface tun1, id 1
    Section number: 1
  > Interface id: 1 (tun1)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:07:57.536175173 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692900477.536175173 seconds
    [Time delta from previous captured frame: 0.044663801 seconds]
    [Time delta from previous displayed frame: 0.557941330 seconds]
    [Time since reference or first frame: 2392.124632056 seconds]
    Frame Number: 19190
    Frame Length: 109 bytes (872 bits)
    Capture Length: 109 bytes (872 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51101, Dst Port: 38435
> Datagram Transport Layer Security
```

16	IR-06	VERIFY	CS DTSR Live Log	Verify the Switchover Time is less than the TET for a Scheduled MbB Switchover	Verify the Switchover time is less than TET for a Scheduled MbB Switchover

UA DTSR:
2023-08-24 18:07:56.977766 GMT INFO   SessionManager.cpp:477   SWITCH completed in 699 ms
CS DTSR:
2023-08-24 18:07:56.758932 GMT INFO   SessionManager.cpp:477   SWITCH completed in 616 ms

A.1.10 TP_CM_010 – Link Switchover > TET with Link Recovery

STEP	REQ	Action	Component	Description	Procedure
1	IR-04	VERIFY	CS Main Sniffer	Verify that User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent by the CS via the link supporting the active Connection

Verification looks the same as step 1 of TP_CM_009; not repeating for conciseness.

STEP	REQ	Action	Component	Description	Procedure
2	IR-04	VERIFY	UA Main Sniffer	Verify that User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received by the UA via the link supporting the active Connection

Verification looks the same as step 2 of TP_CM_009; not repeating for conciseness.

STEP	REQ	Action	Component	Description	Procedure

3	IR-08	OBSERVE	CS LMSF Console	View the status of all available links	`lmsf`
					`lmsf> status`

4	IR-08	OBSERVE	UA LMSF Console	View the status of all available links	`cs-sh lmsf`
					`lmsf> status`

5	IR-05	INVOKE	CS OS Console	Initiate a Switchover for the desired alternate link using a switchover time greater than TET	`disable_link 1`
					`disable_link 2`
					`disable_link 3`

6	IR-05	WAIT	CS Operator	“	Time greater than TET passes

7	IR-05	INVOKE	CS OS Console	“	`enable_link 1`
					`enable_link 2`
					`enable_link 3`

8	IR-08	OBSERVE	CS DTSR Live Log	Status indication that Lost C2 Link state has been declared	Observe notification indicating Lost C2 Link
9	IR-06	OBSERVE	UA DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.
10	IR-06	OBSERVE	CS DTSR Live Log	Observe the Switchover and note the Switchover Time	Verify the start and end timestamps of the Switchover.

11	IR-05
	IR-07
	IR-10
		VERIFY	UA LMSF Console and DTSR Live Log	UA status shows:
				…secure session is established
				…the link has changed to the specified link
				…the UA DTSR indicated an interruption exceeding TET
					`cs-sh lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`
					Indication that interruption was greater than TET

```
2023-09-06 19:55:02.831204 GMT
Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

12	IR-05
	IR-07
	IR-10
		VERIFY	CS LMSF Console and DTSR Live Log	CS status shows:
				…secure session is established
				…the link has changed to the specified link
				…the CS DTSR indicated an interruption exceeding TET
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`
					
					Indication that interruption was greater than TET

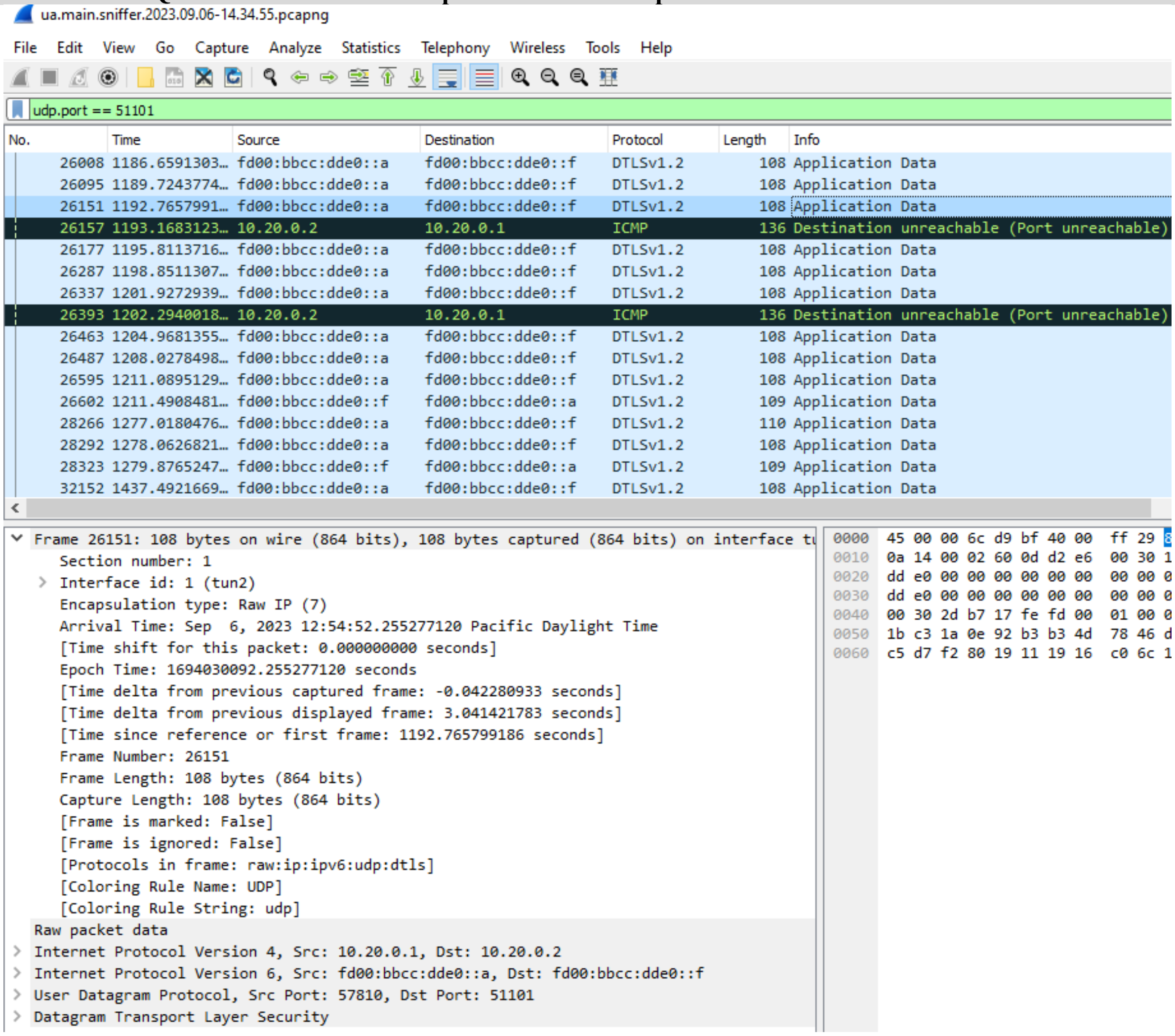
2023-09-06 19:55:12.591624 GMT Secure Link Detailed Status: userOut enabled: 1 controlOut enabled: 1 user plane: CONNECTED control plane: CONNECTED					
13	IR-04 IR-18 IR-19c	VERIFY	CS Main Sniffer	On the CS, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data messages are sent to the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
This verification step looks the same as step 10 of TP_CM_009; not repeating here for conciseness.					
14	IR-04 IR-18 IR-19c	VERIFY	UA Main Sniffer	On the UA, verify: …messages are exchanged over the active link …addresses are unique	Verify via the traffic sniffer log that: a) User Data Messages are received by the UA only via the link supporting the active connection b) all exchanged messages include unique IP source and destination addresses that uniquely identify the UA and CS c) addresses are unique across paths over networked A/G links and over point-to-point A/G links
This verification step looks the same as step 11 of TP_CM_009; not repeating here for conciseness.					
15	IR-20	VERIFY	UA DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages. b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

a) Control messages are shown in UA DTSR log.

```
2023-09-06 19:54:35.911741 GMT LIVE_VALIDATION LinkManager.cpp:213
Lost link for secure connection.  Sending switch command.
Switch timer started
Initiating lost-link switchover0
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 3
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 1
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ          3
Switchover Innitiator Task: sent CONNECT_REQ over link 2
CONTROL PLANE: CONNECT.CNF          4    Accepted[09040001]<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
 Received CONNECT.CNF. New link:
```

b) UA User Sniffer shows DTLS session is maintained for the duration of the connection disruption; no DTLS errors are logged.

STEP	REQ	Action	Component	Description	Procedure



ua.main.sniffer.2023.09.06-14.34.55.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 51101

```
No.      Time              Source              Destination         Protocol  Length Info
   26008 1186.6591303… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26095 1189.7243774… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26151 1192.7657991… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26157 1193.1683123… 10.20.0.2          10.20.0.1          ICMP       136 Destination unreachable (Port unreachable)
   26177 1195.8113716… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26287 1198.8511307… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26337 1201.9272939… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26393 1202.2940018… 10.20.0.2          10.20.0.1          ICMP       136 Destination unreachable (Port unreachable)
   26463 1204.9681355… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26487 1208.0278498… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26595 1211.0895129… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   26602 1211.4908481… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2   109 Application Data
   28266 1277.0180476… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   110 Application Data
   28292 1278.0626821… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
   28323 1279.8765247… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2   109 Application Data
   32152 1437.4921669… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2   108 Application Data
```

```
Frame 26151: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface tu
    Section number: 1
  > Interface id: 1 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Sep  6, 2023 12:54:52.255277120 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1694030092.255277120 seconds
    [Time delta from previous captured frame: -0.042280933 seconds]
    [Time delta from previous displayed frame: 3.041421783 seconds]
    [Time since reference or first frame: 1192.765799186 seconds]
    Frame Number: 26151
    Frame Length: 108 bytes (864 bits)
    Capture Length: 108 bytes (864 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 57810, Dst Port: 51101
> Datagram Transport Layer Security
```

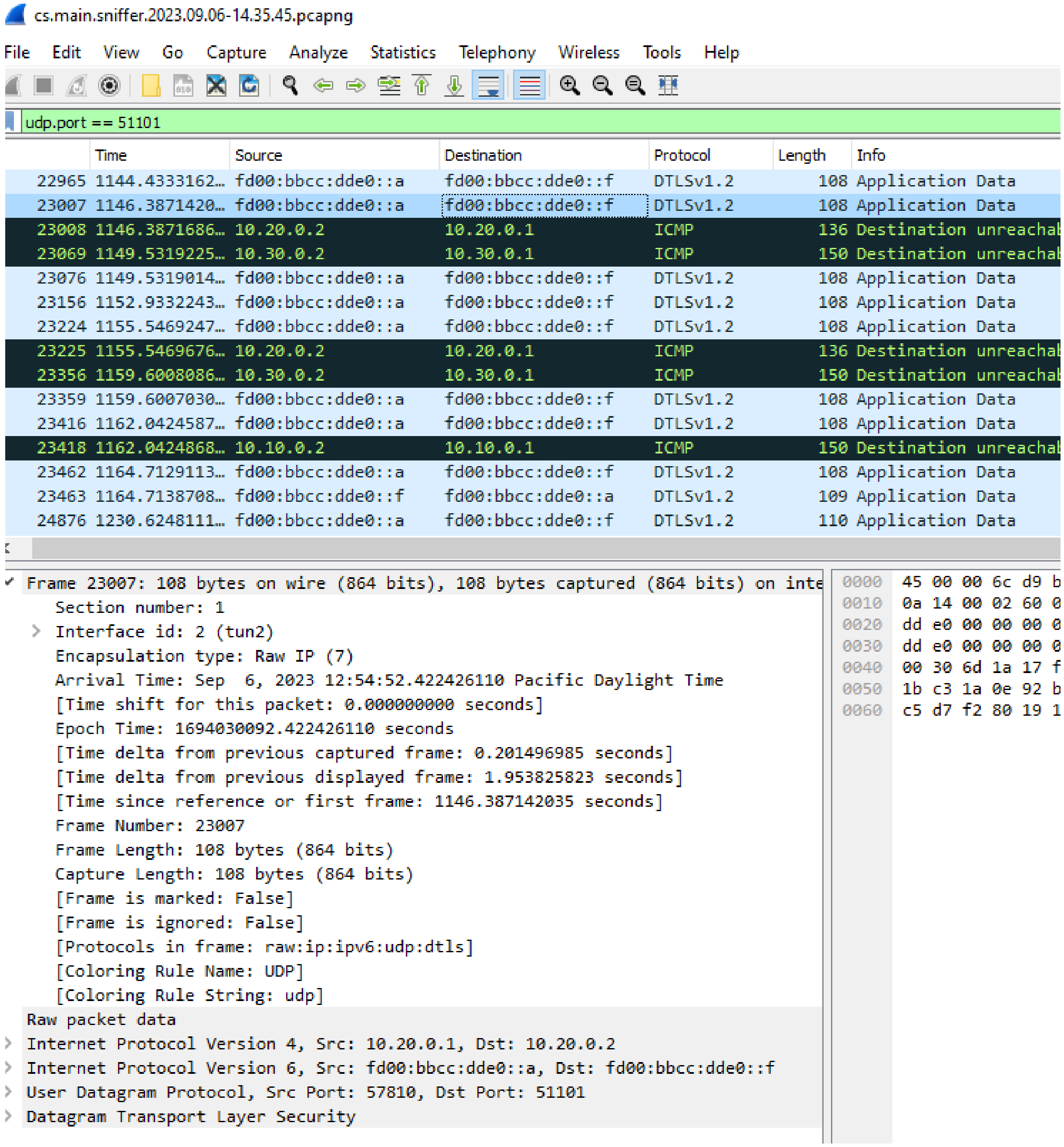
```
0000  45 00 00 6c d9 bf 40 00  ff 29 8
0010  0a 14 00 02 60 0d d2 e6  00 30 1
0020  dd e0 00 00 00 00 00 00  00 00 0
0030  dd e0 00 00 00 00 00 00  00 00 0
0040  00 30 2d b7 17 fe fd 00  01 00 0
0050  1b c3 1a 0e 92 b3 b3 4d  78 46 d
0060  c5 d7 f2 80 19 11 19 16  c0 6c 1
```

16	IR-20	VERIFY	CS DTSR Live Log	Verify the appropriate Control Messages were exchanged while maintaining not breaking the secure connection	Verify via live log that: a) the Control Messages are the appropriate messages for a Network Layer Switchover based on the messages b) the secure connection is maintained (i.e., messages with a DTLS record header are observed, and no DTLS errors are logged)

a) CS DTSR log shows control messages exchanged.

```
2023-09-06 19:54:37.521032 GMT LIVE_VALIDATION LinkManager.cpp:213
Lost link for secure connection.  Sending switch command.
SWITCH timer started
Initiating lost-link switchover0
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ        3
 CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ        3
 CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>[080300]CONNECT.REQ        3
 CONTROL PLANE: CONNECT.REQ          3   Processing suceeded.
CONTROL PLANE: CONNECT.CNF          4    Accepted[09040001]<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

b) CS Main Sniffer shows DTLS session is maintained for the duration of the connection disruption; no DTLS errors are logged.



cs.main.sniffer.2023.09.06-14.35.45.pcapng

udp.port == 51101

```
      Time            Source              Destination         Protocol        Length Info
22965 1144.4333162… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23007 1146.3871420… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23008 1146.3871686… 10.20.0.2           10.20.0.1           ICMP               136 Destination unreachab
23069 1149.5319225… 10.30.0.2           10.30.0.1           ICMP               150 Destination unreachab
23076 1149.5319014… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23156 1152.9332243… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23224 1155.5469247… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23225 1155.5469676… 10.20.0.2           10.20.0.1           ICMP               136 Destination unreachab
23356 1159.6008086… 10.30.0.2           10.30.0.1           ICMP               150 Destination unreachab
23359 1159.6007030… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23416 1162.0424587… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23418 1162.0424868… 10.10.0.2           10.10.0.1           ICMP               150 Destination unreachab
23462 1164.7129113… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           108 Application Data
23463 1164.7138708… fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2           109 Application Data
24876 1230.6248111… fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2           110 Application Data
```

```
✓ Frame 23007: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on inte
     Section number: 1
   > Interface id: 2 (tun2)
     Encapsulation type: Raw IP (7)
     Arrival Time: Sep  6, 2023 12:54:52.422426110 Pacific Daylight Time
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1694030092.422426110 seconds
     [Time delta from previous captured frame: 0.201496985 seconds]
     [Time delta from previous displayed frame: 1.953825823 seconds]
     [Time since reference or first frame: 1146.387142035 seconds]
     Frame Number: 23007
     Frame Length: 108 bytes (864 bits)
     Capture Length: 108 bytes (864 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: raw:ip:ipv6:udp:dtls]
     [Coloring Rule Name: UDP]
     [Coloring Rule String: udp]
  Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.1, Dst: 10.20.0.2
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::a, Dst: fd00:bbcc:dde0::f
> User Datagram Protocol, Src Port: 57810, Dst Port: 51101
> Datagram Transport Layer Security
```

```
0000  45 00 00 6c d9 b
0010  0a 14 00 02 60 0
0020  dd e0 00 00 00 0
0030  dd e0 00 00 00 0
0040  00 30 6d 1a 17 f
0050  1b c3 1a 0e 92 b
0060  c5 d7 f2 80 19 1
```

STEP	REQ	Action	Component	Description	Procedure
17	IR-21	VERIFY	UA Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

The verification for this step looks the same as step 15 from TP_CM_009; not repeating for conciseness.

STEP	REQ	Action	Component	Description	Procedure
18	IR-21	VERIFY	CS Main Sniffer	Verify User Data and Control Messages are exchanged over the new link and stop over the old link	Verify via the traffic sniffer log that: a) User Data and Control Messages begin to be exchanged over the new Link b) no messages flow over the original link

The verification for this step looks the same as step 16 from TP_CM_009; not repeating for conciseness.

STEP	REQ	Action	Component	Description	Procedure
19	IR-06	VERIFY	CS DTSR Live Logs	Verify the Switchover Time is greater than the TET for a Scheduled MbB Switchover	Verify the Switchover time is greater than TET for a Scheduled MbB Switchover

UA DSTR:

```
2023-09-06 19:55:10.981102 GMT SWITCH completed in 35068 ms.  Switchover TET set at 3000 ms.
```

CS DTSR:

```
2023-09-06 19:55:10.748371 GMT SWITCH completed in 33227 ms.  Switchover TET set at 3000 ms.
```

A.1.11 TP_CM_011 – Control Plane and User Plane Traffic Link Termination

STEP	REQ	Action	Component	Description	Procedure

1	IR-07	VERIFY	CS LMSF console	CS status shows:
				…secure session is established
				…which link is providing the connection
					`lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

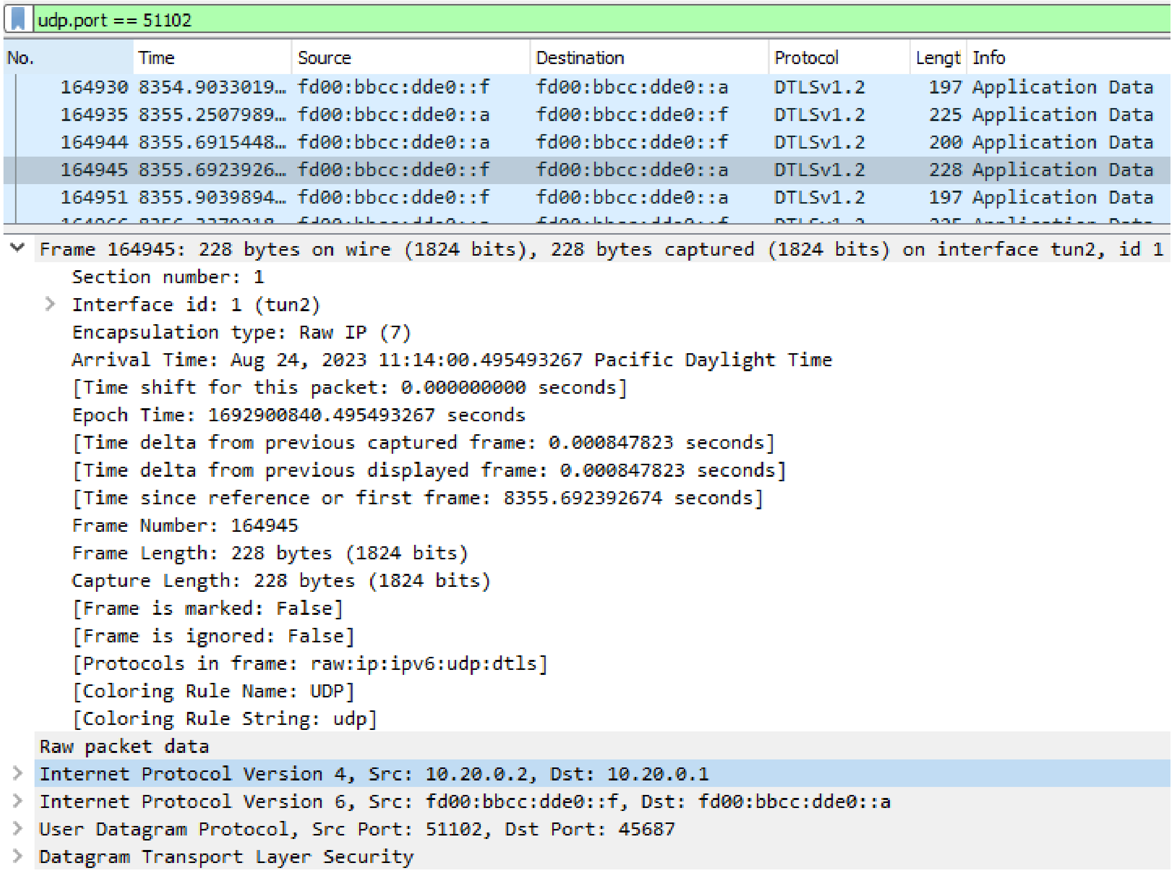
```
2023-08-24 18:15:02.880590 GMT Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

2	IR-07	VERIFY	UA LMSF console	UA status shows:
				…secure session is established
				…which link is providing the connection
					`cs-sh lmsf`
					`lmsf> status secure`
					
					Expected output:
					`STATUS User: Y/<ID> | Control: Y/<ID>`

```
2023-08-24 18:14:34.141313 GMT Secure Link Detailed Status:
userOut enabled: 1
controlOut enabled: 1
user plane: CONNECTED
control plane: CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure
3	IR-04	VERIFY	CS Main Sniffer	User Data is sent over the active link	Verify via the traffic sniffer log that the User Data Messages are only sent to the UA via the link supporting the active Connection

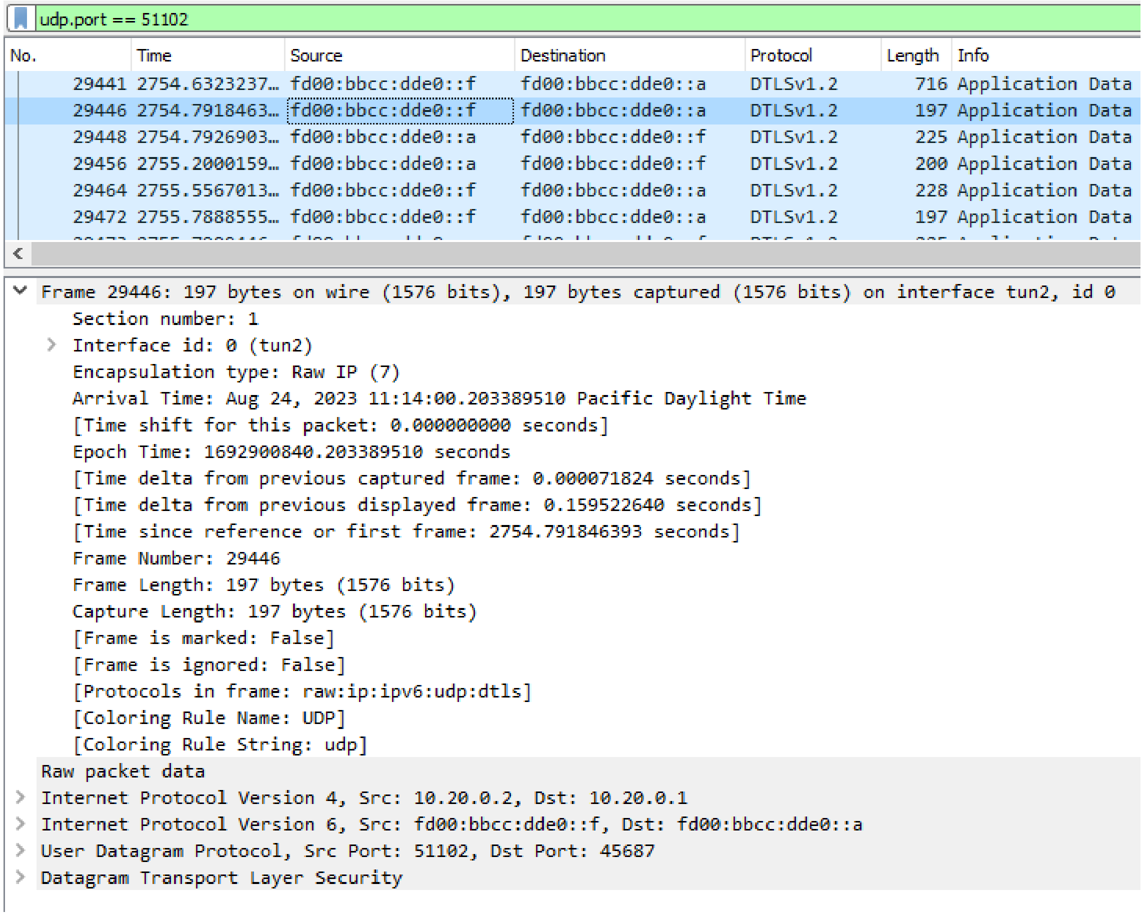


```
udp.port == 51102

No.     Time           Source             Destination        Protocol  Lengt Info
 164930 8354.9033019… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    197 Application Data
 164935 8355.2507989… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    225 Application Data
 164944 8355.6915448… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    200 Application Data
 164945 8355.6923926… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    228 Application Data
 164951 8355.9039894… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    197 Application Data

Frame 164945: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface tun2, id 1
   Section number: 1
 > Interface id: 1 (tun2)
   Encapsulation type: Raw IP (7)
   Arrival Time: Aug 24, 2023 11:14:00.495493267 Pacific Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1692900840.495493267 seconds
   [Time delta from previous captured frame: 0.000847823 seconds]
   [Time delta from previous displayed frame: 0.000847823 seconds]
   [Time since reference or first frame: 8355.692392674 seconds]
   Frame Number: 164945
   Frame Length: 228 bytes (1824 bits)
   Capture Length: 228 bytes (1824 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: raw:ip:ipv6:udp:dtls]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687
> Datagram Transport Layer Security
```

Source 10.20.0.2 is the CS on LTE

4	IR-04	VERIFY	UA Main Sniffer	User Data is received over the active link	Verify via the traffic sniffer log that the User Data Messages are only received via the link supporting the active Connection

STEP	REQ	Action	Component	Description	Procedure



udp.port == 51102

```
No.    Time            Source              Destination         Protocol  Length Info
29441 2754.6323237… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    716 Application Data
29446 2754.7918463… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    197 Application Data
29448 2754.7926903… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    225 Application Data
29456 2755.2000159… fd00:bbcc:dde0::a  fd00:bbcc:dde0::f  DTLSv1.2    200 Application Data
29464 2755.5567013… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    228 Application Data
29472 2755.7888555… fd00:bbcc:dde0::f  fd00:bbcc:dde0::a  DTLSv1.2    197 Application Data
```

```
Frame 29446: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface tun2, id 0
    Section number: 1
  > Interface id: 0 (tun2)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:14:00.203389510 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692900840.203389510 seconds
    [Time delta from previous captured frame: 0.000071824 seconds]
    [Time delta from previous displayed frame: 0.159522640 seconds]
    [Time since reference or first frame: 2754.791846393 seconds]
    Frame Number: 29446
    Frame Length: 197 bytes (1576 bits)
    Capture Length: 197 bytes (1576 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:ipv6:udp:dtls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Raw packet data
> Internet Protocol Version 4, Src: 10.20.0.2, Dst: 10.20.0.1
> Internet Protocol Version 6, Src: fd00:bbcc:dde0::f, Dst: fd00:bbcc:dde0::a
> User Datagram Protocol, Src Port: 51102, Dst Port: 45687
> Datagram Transport Layer Security
```

Destination address 10.20.0.1 is UA on LTE.

5	IR-11	SEND	CS LMSF	Terminate the secure Control Plane traffic and User Plane traffic connection	`lmsf> secure stop`

6	IR-07
	IR-11
		VERIFY	CS LMSF console	CS status shows no secure connection for User Plane traffic or Control Plane traffic	`lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User:` **N**`/<ID> |`
					`Control:` **N**`/<ID>`

```
2023-08-24 18:15:23.648267 GMT INFO    Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

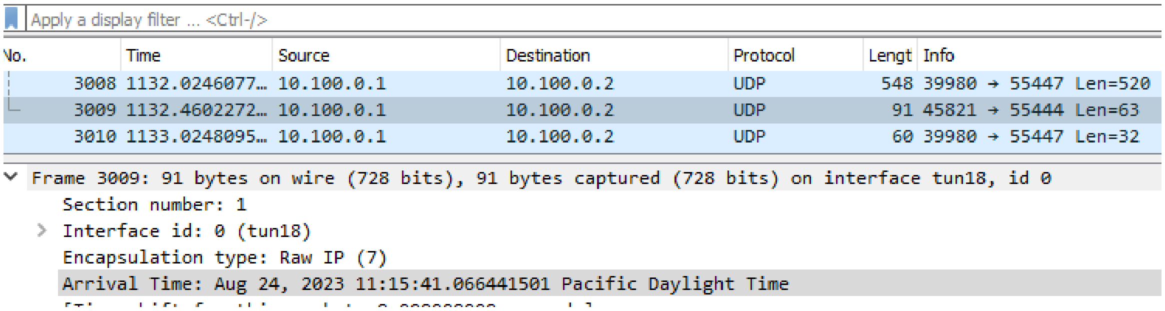
7	IR-07
	IR-11
		VERIFY	UA LMSF console	UA status shows no secure connection for User Plane traffic or Control Plane traffic	`cs-sh lmsf`
					`lmsf> status secure`
					Expected output:
					`STATUS User:` **N**`/<ID> |`
					`Control:` **N**`/<ID>`

```
2023-08-24 18:15:32.307958 GMT Secure Link Detailed Status:
userOut enabled: 0
controlOut enabled: 0
user plane: NOT CONNECTED
control plane: NOT CONNECTED
```

STEP	REQ	Action	Component	Description	Procedure

8	IR-04	SEND	UA UDMD Console	Send User Data	`cs-sh udmd`
					`udmd> send n=1 at 11:15 PDT`

9		VERIFY	UA User Sniffer	UDMD sent a User Data message to DTSR	From the traffic sniffer, verify the User Data message is sent from the UDMD to the DTSR



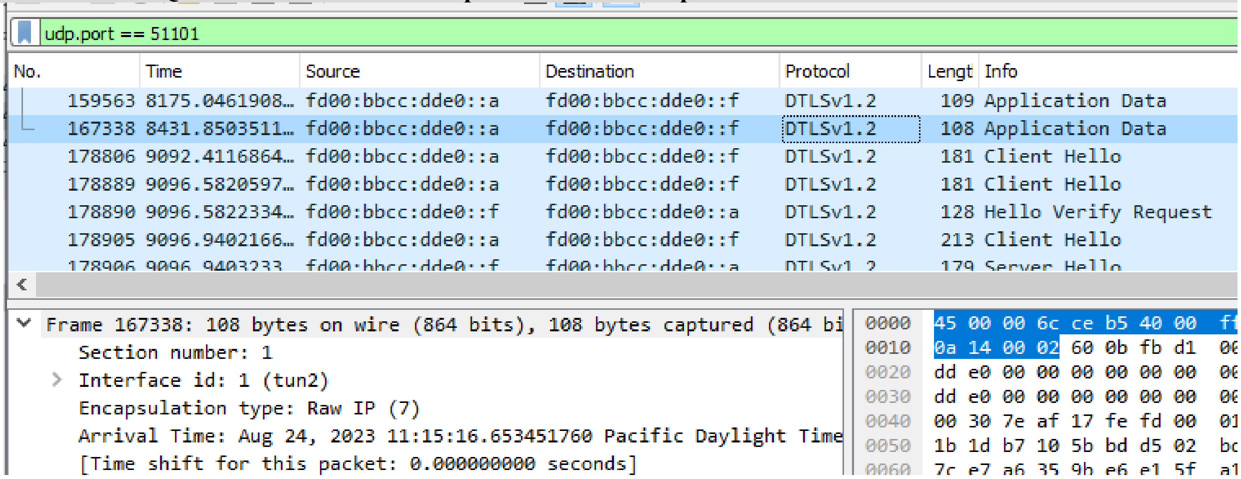
```
Apply a display filter ... <Ctrl-/>

No.   Time             Source       Destination  Protocol  Lengt  Info
3008  1132.0246077…    10.100.0.1   10.100.0.2   UDP       548    39980 → 55447 Len=520
3009  1132.4602272…    10.100.0.1   10.100.0.2   UDP       91     45821 → 55444 Len=63
3010  1133.0248095…    10.100.0.1   10.100.0.2   UDP       60     39980 → 55447 Len=32

Frame 3009: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tun18, id 0
    Section number: 1
  > Interface id: 0 (tun18)
    Encapsulation type: Raw IP (7)
    Arrival Time: Aug 24, 2023 11:15:41.066441501 Pacific Daylight Time
```

STEP	REQ	Action	Component	Description	Procedure
10	IR-04 IR-11	VERIFY	UA Main Sniffer	User Data and Control Messages are not transmitted by the UA DTSR	Verify via the traffic sniffer log that User Data and Control messages are not sent by UA

```
2023-08-24 18:15:41.066531 GMT INFO     UdmdIn.cpp:51
Received: ID: 00000014 Origin: UDMD Cmd: SEND Size: 63 Rsp: FALSE Data:
UD-AAAAAAAAAAAAAAAAAAAA-000014
Secure session disabled - ID: 00000014 Origin: UDMD Cmd: SEND Size: 63 Rsp:
FALSE not sent to peer to lmsf_queue
```

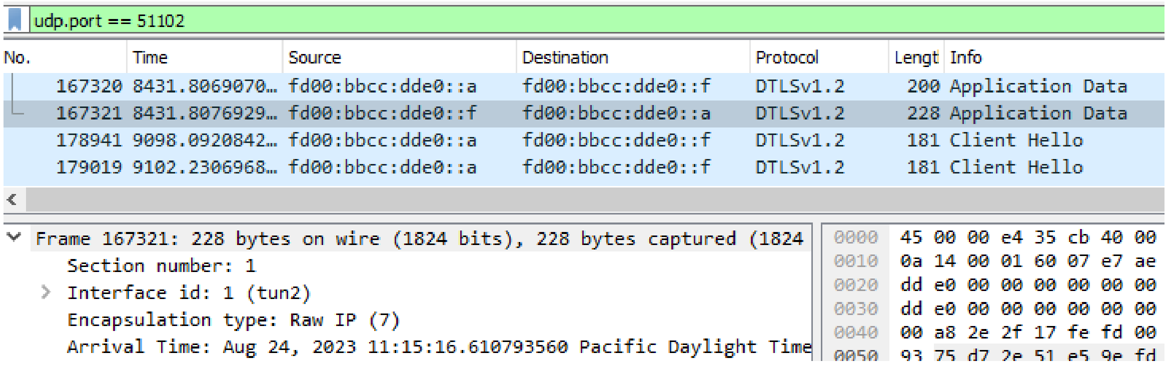
STEP	REQ	Action	Component	Description	Procedure
11	IR-04 IR-11	VERIFY	CS Main Sniffer	User Data and Control Messages are not received by CS DTSR	Verify via the traffic sniffer log that the User Data and Control messages were not received

STEP	REQ	Action	Component	Description	Procedure



```
udp.port == 51101

No.     Time             Source              Destination         Protocol   Lengt Info
 159563 8175.0461908…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    109 Application Data
 167338 8431.8503511…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    108 Application Data
 178806 9092.4116864…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello
 178889 9096.5820597…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello
 178890 9096.5822334…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    128 Hello Verify Request
 178905 9096.9402166…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    213 Client Hello
 178906 9096.9403233   fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    179 Server Hello

Frame 167338: 108 bytes on wire (864 bits), 108 bytes captured (864 bi    0000  45 00 00 6c ce b5 40 00  ff
    Section number: 1                                                    0010  0a 14 00 02 60 0b fb d1  00
  > Interface id: 1 (tun2)                                               0020  dd e0 00 00 00 00 00 00  00
    Encapsulation type: Raw IP (7)                                       0030  dd e0 00 00 00 00 00 00  00
    Arrival Time: Aug 24, 2023 11:15:16.653451760 Pacific Daylight Time  0040  00 30 7e af 17 fe fd 00  01
    [Time shift for this packet: 0.000000000 seconds]                    0050  1b 1d b7 10 5b bd d5 02  bc
                                                                         0060  7c e7 a6 35 9b e6 e1 5f  a1
```

CS Main sniffer shows last control plane message at 11:15:16; next message is 11:26, which is the start of the next scenario.



```
udp.port == 51102

No.     Time             Source              Destination         Protocol   Lengt Info
 167320 8431.8069070…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    200 Application Data
 167321 8431.8076929…  fd00:bbcc:dde0::f   fd00:bbcc:dde0::a   DTLSv1.2    228 Application Data
 178941 9098.0920842…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello
 179019 9102.2306968…  fd00:bbcc:dde0::a   fd00:bbcc:dde0::f   DTLSv1.2    181 Client Hello

Frame 167321: 228 bytes on wire (1824 bits), 228 bytes captured (1824    0000  45 00 00 e4 35 cb 40 00
    Section number: 1                                                    0010  0a 14 00 01 60 07 e7 ae
  > Interface id: 1 (tun2)                                               0020  dd e0 00 00 00 00 00 00
    Encapsulation type: Raw IP (7)                                       0030  dd e0 00 00 00 00 00 00
    Arrival Time: Aug 24, 2023 11:15:16.610793560 Pacific Daylight Time  0040  00 a8 2e 2f 17 fe fd 00
                                                                         0050  93 75 d7 2e 51 e5 9e fd
```

CS Main sniffer shows last user plane message at 11:15:16; next message is at 11:26, which is the start of the next scenario.

12	IR-11	VERIFY	UA DTSR Live Log	Connection termination Control Messages have been exchanged between the UA and CS	Verify connection termination Control messages have been exchanged

```
2023-08-24 18:15:16.664426 GMT INFO     LmsfIn.cpp:129
Received ID: 00000016 Origin: LMSF Cmd: SECURE Size: 40 Rsp: FALSE Arg: 0
Forwarding ID: 00000016 Origin: LMSF Cmd: SECURE Size: 40 Rsp: FALSE Arg: 0
to control_plane
Secure Stop received from LMSF - notifying peer
Sent "USER_DISCONNECT.REQ     3    " across secure connection
Disabling secure session
```

13	IR-11	VERIFY	CS DTSR Live Log	Connection termination Control Messages have been exchanged between the UA and CS	Verify connection termination Control messages have been exchanged

```
2023-08-24 18:15:16.653621 GMT INFO
Received "USER_DISCONNECT.REQ     3    " over secure session
Disabling secure session
```

B. INSPECTION RESULTS – UAS C2 LINK SYSTEM SECURITY

The following table summarizes the MASPS security requirements for which the Detailed Test Procedures [DTP] include an INSPECTION and/or VERIFY test step as a means to show compliance with the MOC in [DO-377A] for the UAS C2 Link System security. Note that the table includes pairs of requirements, e.g., SER-01 and SER-08, where the same MOC and inspection test step action are applicable to the respective security requirements for User Plane traffic and Control Plane traffic exchanged between the UA DTSR and the CS DTSR.

Table B-1 – Security Requirements with an INSPECTION or VERIFY Test Step

DO-377A			[DTP]
Req. No:	**Requirement**	**Means of Compliance (MOC)**	**Test Procedure and Test Step**
SER-01	The UAS C2 Link security system **shall** provide mutual peer entity authentication of C2 User Plane traffic between the UA and CS.	FIPS 140-2 Annex D key establishment and authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A**, Step 1 **TP_CM_001**
SER-08	The UAS C2 Link security system **shall** provide mutual peer entity authentication of C2 Control Plane traffic between the UA and CS.		
SER-02	The UAS C2 Link security system **shall** provide data origin authentication of C2 User Plane traffic between the UA and CS.	AES Counter with CBC-MAC (CCM) per NIST SP 800-38C, or AES Galois Counter Mode (GCM) per NIST SP 800-38D, or Keyed-Hash Message Authentication Code (HMAC) per FIPS PUB. 198-1 with an authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A,** Step 1 **TP_CM_005A**, Step 4
SER-09	The UAS C2 Link security system **shall** provide data origin authentication of C2 Control Plane traffic between the UA and CS.		**IP_CM_001A,** Step 1 **TP_CM_008**, Step 3
SER-03	The UAS C2 Link System security **shall** provide data integrity and anti-replay protection fir C2 User Plane traffic between the UA and CS,	AES-CCM per NIST SP 800-38C, or AES-GCM per NIST SP 800-38D, or HMAC per FIPS PUB. 198-1 with an authentication tag of at least 64 bits or equivalent MOC.	**IP_CM_001A,** Step 1 **TP_CM_005A**, Step 4
SER-10	The UAS C2 Link System security **shall** provide data integrity and anti-replay protection fir C2 Control Plane traffic between the UA and CS,		**IP_CM_001A,** Step 1 **TP_CM_008**, Step 3
SER-04	The UAS C2 Link security system **shall** provide confidentiality of sensitive C2 User Plane traffic between the UA and CS.	AES-CCM per NIST SP 800-38C, or AES-GCM per NIST SP 800-38D or equivalent MOC.	**IP_CM_001A**, Step 1 **TP_CM_004**
SER-11	The UAS C2 Link security system **shall** provide confidentiality of sensitive C2 Control Plane traffic between the UA and CS.		**IP_CM_001A**, Step 1 **TP_CM_007**
SER-05	The UAS C2 Link security system **shall** use cryptographic algorithms, with algorithm strength and key length sufficient to protect C2 User Plane traffic between the UA and CS for the duration of a flight.	Meet algorithm strength and key length requirements of NIST SP 800-131A, Rev. 2, or equivalent MOC. SP 800-131A recognizes that large-scale quantum computers, when available, will threaten the security of NIST-approved public key algorithms.	**IP_CM_001A**, Step 1
SER-12	The UAS CS C2 Link security system **shall** use cryptographic algorithms with algorithm strength and key length sufficient to protect C2 Control Plane traffic between the UA and CS.		**IP_CM_001A**, Step 1

Section B.1 summarizes the cryptographic configuration including the key characteristics of the selected cryptographic library, the cryptographic library build used for the validation tests, and the application configurations (cipher suites) used for the validation tests. Section B.2 references the cryptographic configuration and provide the inspection results for each of the requirement pairs identified in Table B-1.

B.1 CRYPTOGRAPHIC CONFIGURATION INSPECTION

B.1.1 Cryptographic Library Characteristics

The UA and CS systems under test leverage the commercial off-the-shelf (COTS) wolfSSL cryptographic library (version 4.4), which supports industry-standard Transport Layer Security (TLS, up to the current version 1.3) and Datagram Transport Layer Security (DTLS, version 1.2) protocols. The UA and CS systems use the DTLS protocol since UDP/IP was selected for the transport/network layers.

The wolfSSL library includes the wolfCrypt library, which provides the underlying cryptographic algorithms used by the TLS/DTLS protocols. The version of wolfSSL selected for this project includes a wolfCrypt library that has been FIPS 140-2 certified (Certificate #3389) under the NIST Crypto Module Validation Program (CMVP). In addition, the individual wolfCrypt cryptographic algorithm implementations have been certified under NIST Crypto Algorithm Validation Program (CAVP), as summarized in the following table.

Table B-2 – wolfCrypt Cryptographic Algorithms and associated NIST CAVP Certificates

Algorithm	Use	Characteristics	Relies on	NIST Reference	NIST CAVP
AES	Encryption/decryption	Key Sizes: 128, 192, 256 Modes: —CBC, CTR, ECB (SP 800-38A) —CMAC (SP 800-38B) —CCM (SP 800-38C) —GCM, GMAC (SP 800-38D) Tag Length: 96, 104, 112, 120, 128	DRBG	FIPS 197	5446
CVL (KAS)	Key agreement	Curves: P-256, P-384, P-521	ECDSA, DRBG, SHS	SP 800-56A	1891
DRBG	Random bit generation	SHA-256-based	SHS	SP 800-90A	2131
ECDSA	Key generation Key verification Signature generation Signature verification	Curves: P-256, P-384, P-521 Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHS, DRBG	FIPS 186-4	1451
KDF	Key Derivation Function	Mode: HMAC-based pseudo-random function (PRF) Hash: SHA-256 or SHA-384	HMAC, SHS	SP 800-56C	Note 1
HMAC	Message authentication code generation and verification	Mode: Hashed Message Authentication Code Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHS	FIPS 198	3604
SHS	Message digest generation	Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	None	FIPS 180	4365
Note 1: The vendor (wolfSSL) affirms conformance of this function to NIST SP 800-56C. This KDF is approved for use within an approved key establishment scheme but the CMVP does not currently provide CAVP component testing. [REF-3389SP]					

Certificate #3389 and the associated CAVP certificates cover operating environments (i.e., operating system plus computing platform) that are similar to the UA operating environment (i.e., Ubuntu Linux running on an ARM v8 processor) and the CS operating environment (i.e., Ubuntu Linux running on an Intel CPU). As documented previously in the [SRS], formal FIPS validation per SER-06 / SER-13 is out-of-scope of this project. However, the information presented in this section is intended to show that there is a path to FIPS validation for future production UA and CS systems using existing COTS crypto libraries.

B.1.2 Cryptographic Library Build

Panel A in the following figure lists the contents of the Config.sh file, which enables option settings for the wolfSSL cryptographic library build. Panel B is a configuration summary output file that was generated by the wolfSSL library at the time of build for the UA and CS. Since the same cryptographic build file is used for both the UA and the CS, the configuration summaries are identical for both systems.

```
#!/bin/bash
RC=0
WORKING_DIR="."
OPTIONS="\
--enable-ipv6 \
--enable-harden \
--enable-fips=v2 \
--enable-opensslextra \
--enable-keygen \
--enable-certgen \
--enable-certreq \
--enable-supportedcurves \
--enable-eccshamir \
--enable-ecc \
--enable-ecccustcurves \
--enable-eccencrypt \
--enable-sha384 \
--enable-dtls \
--enable-dtls-mtu \
--enable-tls13 \
--enable-aes \
--enable-asn \
--enable-testcert \
--enable-nullcipher \
--enable-x963kdf‟
```

A. Config.sh Build File

```
Configuration summary for wolfssl version 4.4.0
*  Installation prefix:        /usr/local
*  System type:                pc-linux-gnu
*  Host CPU:                   x86_64
*  C Compiler:                 gcc
*  AES:                        yes
*  AES-CBC:                    yes
*  AES-GCM:                    yes
*  AES-CCM:                    yes
*  AES-CTR:                    yes
*  DES3:                       yes
*  NULL Cipher:                yes
*  SHA:                        yes
*  SHA-224:                    yes
*  SHA-384:                    yes
*  SHA-512:                    yes
*  keygen:                     yes
*  certgen:                    yes
*  certreq:                    yes
*  Hash DRBG:                  yes
*  PWDBASED:                   yes
*  HKDF:                       yes
*  X9.63 KDF:                  yes
*  DH:                         yes
*  DH Default Parameters:      yes
*  ECC:                        yes
*  ECC Custom Curves           yes
*  ECC_ENCRYPT:                yes
*  DTLS:                       yes
*  TLS v1.3:                   yes
*  Supported Elliptic Curves:  yes
*  Extended Master Secret:     yes
```

B. Configuration Summary Output

B-1 – wolfSSL Cryptographic Library Build

These figures will be referenced as necessary in the detailed inspection results in Section B.3.

B.1.3 Application Configurations

Two UA and CS DTSR application configurations were employed to support tests of the UAS C2 security requirements:

- **AEAD Configuration** – Uses the cipher suite `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)`. This configuration, which uses AES in the GCM operating mode with 256-bit keys, was used to demonstrate compliance with the confidentiality requirements in SER-04 and SER-11.
- **NULL Configuration** – Uses the cipher suite `TLS_ECDHE_ECDSA_WITH_NULL_SHA (0xC0, 0x06)`. This configuration, which uses the NULL confidentiality algorithm (i.e., no encryption), was used to demonstration compliance with all SER requirements with the exception of the confidentiality requirements in SER-04 and SER-11.

  Note: The cipher suites are registered on the IANA web site, and the pair of hexadecimal values shown above in parentheses are an index into the table of registered values.

With the exception of the confidentiality algorithm (AES vs. NULL) and the hash function (SHA384 vs. SHA), the other algorithms in the cipher suites are identical (i.e., TLS, ECDHE, ECDSA). When using the AEAD Configuration, the AES_256_GCM algorithm provides authenticated encryption, which simultaneously provides both confidentiality and authenticity of the data. Since the AEAD algorithm performs authentication-then-encryption (i.e., the authentication tag is computed first, then both the plaintext data and the authentication tag are encrypted), the encrypted authentication tag cannot be observed directly (i.e., from a "black box" test perspective) in message exchanges. Therefore, the NULL Configuration was employed for validating the security requirements (e.g., SER-01/SER-08) where observing the authentication tag/length is specified in the means of compliance.

B.2 SECURITY REQUIREMENT INSPECTION

B.2.1 SER-01 / SER-08 Compliance

The MOC for SER-01/SER-08 references NIST FIPS 140-2 Annex D [REF-140-2], which specifies approved key establishment techniques. The listed techniques include NIST SP 800-56A [REF-56A], Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. Section 10 of NIST SP 800-56A states that an implementation claiming conformance must show use of:

- Elliptic Curve (EC) cryptography plus use of a NIST-recommended elliptic curve.
- Approved key agreement scheme
- Approved hash function
- Approved random bit generation
- Approved key generation scheme
- Approved key derivation function
- A MAC tag length greater than or equal to 64 bits (for all elliptic curve sizes and domain parameters).

The cipher suites for both the AEAD and NULL application configurations specify Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), which is an approved key agreement scheme per NIST SP 800-56A, and the selected elliptic curves (secp521r1 for the NULL Configuration and secp256r1 for the AEAD Configuration) meet the NIST SP 800-131A Rev.2 minimum length/strength requirements. Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library implements the CVL Key Agreement Scheme (KAS) per NIST SP 800-56A and was certified under the NIST CAVP (certificate number 1891). The CVL KAS also uses an approved hash (SHS) per NIST FIPS 180, approved random bit generation (DRBG) per NIST SP 800-90A, key pair generation per NIST FIPS 186-4, and HMAC-based key derivation function per NIST SP 800-56C. In addition, conformance of CVL KAS with NIST SP 800-56A means that the resulting MAC tag is greater than or equal to 64 bits.

Result = PASS: This inspection demonstrates that the cryptographic module implements a key establishment scheme and associated MAC tag that are compliant with NIST FIPS 140-2 Appendix D and the key establishment technique specified in NIST SP 800-56A.

B.2.2 SER-02 / SER-09 and SER-03 / SER-10 Compliance

B.2.2.1 AEAD APPLICATION CONFIGURATION

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the AES algorithm in accordance with NIST FIPS 197 operating in the AES-GCM mode per NIST SP 800-38D. Key lengths of 128, 192, and 256 bits are supported, and the registered cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the use of AES-GCM with 256-bit keys.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-aes \` option, and the configuration summary shown in Panel B confirms that the AES algorithm and the AES-GCM mode of operation are configured in the UA and CS builds. The AES-GCM mode produces a non-truncated 128-bit (16 byte) authentication tag.

Result = PASS: This inspection demonstrates that the cryptographic module was configured for AES with an approved symmetric key block cipher mode (AES-GCM per NIST SP 800-38D), which produces a non-truncated 128-bit (16 byte) authentication tag that is compliant with the MOC for SER-02 / SER-09 and SER-03 / SER-10.

B.2.2.2 NULL APPLICATION CONFIGURATION

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the Hashed Message Authentication (HMAC) function in accordance with NIST FIPS 198 with an underlying Secure Hash Standard (SHS) algorithm in accordance with NIST FIPS 180.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-nullcipher \` option, and the configuration summary shown in Panel B confirms that the NULL Cipher is configured in the UA and CS builds. The registered NULL cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`NULL_SHA`**) invokes the use of HMAC with the SHA-1 hash algorithm, which produces a non-truncated 160-bit (20-byte) authentication tag.

Result = PASS: This inspection demonstrates that the cryptographic module was configured for HMAC-SHA1 per NIST FIPS 198 and produces a 160-bit tag, which is compliant with the MOC for SER-02/SER-09 and SER-03/SER-10.

B.2.3 SER-04 / SER-11 Compliance

The tests procedures used to validate the SER-04 and SER-11 confidentiality requirement used the AEAD Configuration. In this configuration, the registered cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the AES algorithm operating in the GCM mode with 256-bit keys.

Per Section B.1.1, the FIPS-validated wolfSSL wolfCrypt library supports the AES algorithm in accordance with NIST FIPS 197 operating in the AES-GCM mode per NIST SP 800-38D. Key lengths of 128, 192, and 256 bits are supported, and the selected cipher suite (`TLS_ECDHE_ECDSA_WITH_`**`AES_256_GCM`**`_SHA384`) invokes the use of AES-GCM with 256-bit keys.

As shown in Panel A of the figure in B.1.2, the build file includes the `--enable-aes \` option, and the configuration summary shown in Panel B confirms that the AES algorithm and the AES-GCM mode of operation are configured in the UA and CS builds.

Result = PASS: This inspection demonstrates that the cryptographic module was configured for AES using an approved symmetric key block cipher mode (AES-GCM per NIST SP 800-38D), which is compliant with the MOC for SER-04 / SER-11.

B.2.4 SER-05 / SER-12 Compliance

This section summarizes UA and CS cryptographic module compliance with the algorithm, strength, and key length requirements per NIST SP 800-131A, Rev. 2. In the following table, the first two columns enumerate the algorithm-specific requirements contained in the NIST document. The remaining columns summarize compliance, including:

- **wolfSSL Crypto Library** – A yes (Y) or no (N) compliance indication and a pointer to the algorithm row in Table 4-13 that provides specific details and NIST CAVP certificates.
- **UA and CS Prototype Implementation** – A yes (Y) or no (N) compliance indication and the specific algorithm, mode, key length used in the prototype for each of the two application configurations (AEAD, NULL).

Table B-3 – Compliance with NIST SP 800-131A, Rev. 2

NIST SP 800-131A, Rev.2		**Compliance**		
Section – Algorithm	**Requirement(s)**	**wolfSSL Crypto Library per Table 4-13**	**UA and CS Prototype Implementation (reference Section 4.5.1.3)**	
			AEAD Configuration	**NULL Configuration**
2 – Encryption and Decryption using Block Cipher Algorithms	• AES per NIST FIPS 197 • 128, 192, or 256-bit keys • Approved mode of operation per NIST SP 800-38 series	**Y** AES	**Y** AES-256-GCM	**Not applicable** – NULL encryption
3 – Digital Signature	• DSA per NIST FIPS 186-4 • ECDSA len(n) >= 224	**Y** ECDSA	**Y** ECDSA using P-521 curve and SHA-512 (**Note 1**)	**Y** ECDSA using P-521 curve and SHA-512 (**Note 1**)
4 – Random Bit Generation	• DRBG per SP 800-90A	**Y** DRBG	**Y** Hash_DRBG using SHA-256	**Y** Hash_DRBG using SHA-256
	• Hash_DRBG or HMAC_DRBG using any hash per NIST FIPS 180	**Y** SHS		
5 – Key Agreement using Diffie-Hellman (DH)	• Diffie-Hellman per NIST SP900-56A • DH >= 112 bits of security (i.e., len(n) >= 224).	**Y** CVL (KAS)	**Y** ECDH-E using P-256 curve (**Note 1**)	**Y** ECDH-E using P-521 curve (**Note 1**)
6 – Key Agreement using RSA			**Not applicable** – UA and CS prototypes use Diffie-Hellman key agreement in lieu of RSA; refer to previous row.	
7 – Key Wrapping			**Not applicable** – Key wrapping not required for the UA and CS prototype implementations.	
8 – Deriving Additional Keys from a Crypto-graphic Key	• HMAC per FIPS 198 or • CMAC per SP 800-38B plus AES-128 per FIPS 197	**Y** KDF	**Y** HMAC-SHA-384	**Y** HMAC-SHA-256

NIST SP 800-131A, Rev.2		Compliance		
Section – Algorithm	**Requirement(s)**	**wolfSSL Crypto Library per Table 4-13**	**UA and CS Prototype Implementation (reference Section 4.5.1.3)**	
			AEAD Configuration	**NULL Configuration**
	• Key derivation key >= 112 bits		(**Note 2**)	(**Note 2**)
9 – Hash Functions	• Secure hash algorithm per NIST FIPS 180	**Y** SHS	**Y** SHA-256 (DRBG) SHA-384 (KDF) SHA-512 (ECDSA)	**Y** SHA-1 (HMAC, **Note 3**) SHA-256 (DRBG, KDF) SHA-512 (ECDSA)
	• SHA-224, -256, -384, -512 acceptable			
10 – Message Authentication Codes	• HMAC per FIPS 198; or • CMAC per SP 800-38B plus AES-128 per FIPS 197; or • GMAC per SP 800-38D plus AES-128 per FIPS 197; or • KMAC per SP 800-185 plus SHA3 per FIPS 202	Y GCM/GMAC plus AES	**Y** AES-256-GCM	Not applicable
		Y HMAC	Not applicable	**Y** HMAC-SHA1-160 (**Note 3**)

NOTES:

1. For each case, the selected curve meets the NIST SP 800-131A Rev.2 minimum length/strength requirements.

2. Per RFC 5246 [REF-5246], TLS v1.2 specifies the use of an HMAC-based pseudo-random function with SHA-256, unless a stronger hash is specified, to generate symmetric keys for message authentication and confidentiality.

3. Per NIST SP 800-131A Rev.2, any approved hash algorithm per NIST FIPS 180-4, which includes SHA-1, may be used for HMAC as long as the key size is greater than 112 bits.

Result = **PASS**: This inspection demonstrates that the cryptographic module was configured to use algorithms with strength and key length requirements per NIST SP-800-131A, Rev. 2 in compliance with the MOC for SER-05 / SER-12.

C. INSPECTION RESULTS – VPN FOR PROTECTING THE UA-TO-C2CSP AND C2CSP-TO-CS COMMUNICATION LINKS

The UA and CS systems under test implement a VPN that provides protections to satisfy the following DO-377A MASPS security requirements:

- **SER-14** (User Plane traffic) – Air/ground network connection between the CS and C2CSP secured in accordance with SER-01 through SER-06[1].
- **SER-15** (User Plane traffic) – Air/ground network connection between the UA and C2CSP secured in accordance with SER-01 through SER-06.
- **SER-16** (Control Plane traffic) – Air/ground network connection between the CS and C2CSP secured in accordance with SER-08 through SER-13.
- **SER-17** (Control Plane traffic) – Air/ground network connection between the UA and C2CSP secured in accordance with SER-08 through SER-13.

As documented previously in the [SRS], formal FIPS validation per SER-06 / SER-13 is out-of-scope of this project. Therefore, the inspection of SER-14 / SER-15 requirements considers only SER-01 through SER-05, and the inspection of SER-16 / SER-17 considers only SER-08 through SER-12. As described previously in Appendix B of this report, the inspection examines pairs of requirements, e.g., SER-01 and SER-08, where the security requirements for User Plane traffic and Control Plane traffic specify the same MOC. Refer to Table B-1 in Appendix B of this report for the requirement text and MOCs for the applicable security requirements.

Section C.1 summarizes the cryptographic characteristics of the selected VPN, and Section C.2 provide the inspection results for each of the requirement pairs identified previously in Table B-1.

C.1 CRYPTOGRAPHIC CONFIGURATION INSPECTION

C.1.1 CRYPTOGRAPHIC CHARACTERISTICS

The UA and CS systems under test leverage the commercial off-the-shelf (COTS) WireGuard® VPN software to protect both User Plane and Control Plane traffic exchanged between the UA and CS via the UA-to-C2CSP and C2CSP-to-CS communication links. WireGuard VPN is open source software (i.e., GLPv2 license similar to OpenVPN) that employs start-of-the-art cryptography as described in a WireGuard whitepaper [WG-VPN]. Many commercial VPN service providers leverage WireGuard as the underlying VPN protocol; the list of service providers include NordVPN®, Surfshark®, ProtonVPN, VyprVPN™, MozillaVPN®, and dozens more.

The WireGuard VPN implementation uses the single cipher suite `Noise_IKpsk2_25519_ ChaChaPoly_BLAKE2s`. Although the underlying crypto-algorithms used by WireGurad are not certified under the NIST Crypto Algorithm Validation Program (CAVP), the algorithms are specified in industry-standard Internet RFCs, as summarized in the following table:

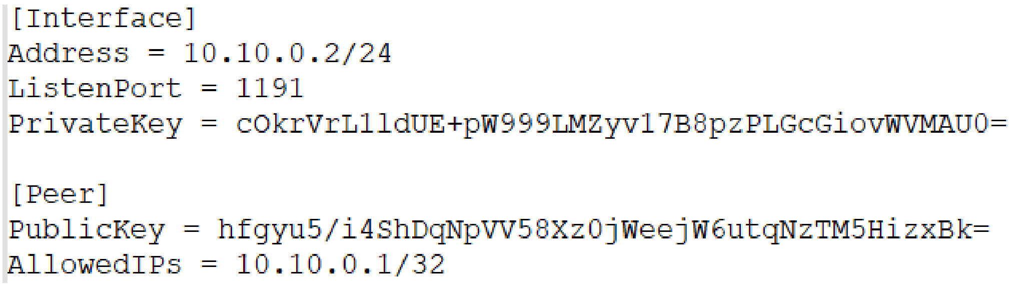
[1] For User Plane traffic, the SER-14 / SER-15 requirements in DO-377A specify compliance with SER-01 through SER-07. In feedback provided previously to the FAA and RTCA SC-228, Honeywell proposed removing the reference to SER-07 since it not practical for air-ground and ground-ground network connections to enforce access controls between the UA and CS C2 Link Management Systems. This proposal was accepted and the draft DO-377B MASPS removes SER-07 from SER-14 / SER-15, which now specify compliance with SER-01 through SER-06.

Table C-1 – WireGuard Cryptographic Algorithms

Algorithm	Use	Characteristics	Standard
ChaCha20-Poly1305	Encryption/decryption with Authentication	Key Size: 256 bits Mode: AEAD Tag Length: 128 bits	RFC 8439
ECDH	Key Agreement	Curve: Curve25519 (256-bit key)	RFC 8418 (ECDH) RFC 7748 (curve)
KDF	Key Derivation Function	Mode: HMAC-based Hash: BLAKE2	RFC 5869
HMAC	Message authentication code generation and verification	Mode: Hashed Message Authentication Code Hash: BLAKE2	RFC 2104
Hash	Message digest generation	Hash: BLAKE2	RFC 7693

C.1.2 VPN CONFIGURATION

Figure 0-1 shows the server configuration used during test flights for the WireGuard VPN software.



```
[Interface]
Address = 10.10.0.2/24
ListenPort = 1191
PrivateKey = cOkrVrL1ldUE+pW999LMZyv17B8pzPLGcGiovWVMAU0=

[Peer]
PublicKey = hfgyu5/i4ShDqNpVV58Xz0jWeejW6utqNzTM5HizxBk=
AllowedIPs = 10.10.0.1/32
```

Figure 0-1: WireGuard VPN Software Configuration (Satcom Link)

C.2 SECURITY REQUIREMENT INSPECTION

C.2.1 SER-01 / SER-08 Compliance

The MOC for SER-01/SER-08 references NIST FIPS 140-2 Annex D [REF-140-2], which specifies approved key establishment techniques. The listed techniques include NIST SP 800-56A [REF-56A], Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. In the following table, the leftmost column summarizes the requirements that must be met to claim conformance with Section 10 of NIST SP 800-56A, and the rightmost columns indicate WireGuard VPN compliance, with support comments as necessary:

Table C-2 – Compliance with NIST SP 800-56A

NIST SP 800-56A	Compliance	
Requirement	WireGuard VPN	Comments
Elliptic Curve (EC) cryptography plus use of a NIST-recommended elliptic curve	Y	WireGuard VPN uses Elliptic Curve Cryptography with Curve25519, which is a NIST-recommended curve per SP800-186. Curve25519 uses a 256-bit key which provideS 128 bits of security, similar to the secp256r1 curve that is used for the C2 Link System (DTSR-to=DTSR) security.
Approved key agreement scheme	Y	WireGuard VPN uses ECDH for key agreement,

NIST SP 800-56A	Compliance	
Requirement	**WireGuard VPN**	**Comments**
Approved hash function	N	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function. The BLAKE2 algorithm is not a NIST-approved hash algorithm; HOWEVER, it was one of the top 5 finalists out of a field of 51 entrants for the NIST hash competition.
Approved random bit generation	N	WireGuard uses the Noise framework for random bit generation, which relies on the /dev/random and /dev/urandom devices under Linux (Ubuntu and Raspberry PI OS). The kernel uses a ChaCha20-based cryptographic pseudorandom number generator that is not NIST-approved.
Approved key derivation function	N	WiredGuard VPN uses an HMAC-based key derivation function per RFC 5869, but the underlying BLAKE2 hash algorithm is no a NIST-approved algorithm.
A MAC tag length greater than or equal to 64 bits (for all elliptic curve sizes and domain parameters)	Y	WireGuard VPN generates HMAC tags that are 128 bits in length, which exceeds the 64-bit requirement,

Result = **PARTIAL**: This inspection shows that WireGuard is partially compliant with the key establishment scheme and associated MAC tag requirements in NIST FIPS 140-2 Appendix D.

C.2.2 SER-02 / SER-09 and SER-03 / SER-10 Compliance

Per Section B.1.1, the WireGuard VPN implementation uses the ChaCha20 encryption algorithm with Poly1305 authenticator to provide authenticated encryption with associated data (AEAD). The encryption key size is 256 bits, which provides 128 bits of security, the same as AES256. ChaCha20-Poly1305 produces a non-truncated 128-bit (16 byte) authentication tag, which is the same length as the tag produced by AES256 operating in GCM mode.

Note that the ChaCha20 and Poly1305 algorithms are specified in cipher suites (e.g., `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256` registered on the IANA web site) for use with TLS v1.2 or DTLS v1.2 (or later versions) per RFC 7905. This demonstrates industry confidence in the security robustness of these algorithms.

Result = **PASS**: This inspection demonstrates that the WireGuard VPN implementation uses an AEAD mode and produces a non-truncated 128-bit (16 byte) authentication tag that satisfies the MOC equivalency for SER-02 / SER-09 and SER-03 / SER-10.

C.2.3 SER-04 / SER-11 Compliance

The MOC for SER-04 / SER-11 specify AES-CCM or AES-GCM, both of which provide AEAD, as an acceptable MOC. As reported in Appendix B in this report, the C2 Link System (DTSR-to-DTSR) security implementation uses AES-GCM with 256-bit keys, which provides 128 bits of security.

Similarly, the WireGuard VPN implementation uses the ChaCha20 encryption algorithm with Poly1305 authenticator to provide AEAD. The encryption key size is 256 bits, which provides 128 bits of security, the same as AES256. ChaCha20-Poly1305 produces a non-truncated 128-bit (16 byte) authentication tag, which is the same length as the tag produced by AES256 operating in GCM mode. As noted in the previous section, the ChaCha20 and Poly1305 algorithms are specified for use with TLS/DTLS.

Result = **PASS**: This inspection demonstrates that the WireGuard VPN implementation uses an authenticated encryption mode that provides data confidentiality with 128 bits of security and that satisfies the MOC equivalency for SER-04 / SER-11.

C.2.4 SER-05 / SER-12 Compliance

This section summarizes WireGuard VPN compliance with the algorithm, strength, and key length requirements per NIST SP 800-131A, Rev. 2. In the following table, the first two columns enumerate the algorithm-specific requirements contained in the NIST document, the last two columns indicate WireGuard VPN compliance, with support comments as necessary.

Table B-3 – Compliance with NIST SP 800-131A, Rev. 2

NIST SP 800-131A, Rev.2		Compliance	
Section – Algorithm	**Requirement(s)**	**WireGuard VPN**	**Comments**
2 – Encryption and Decryption using Block Cipher Algorithms	• AES per NIST FIPS 197	**N**	WireGuarf VPN uses the ChaCha20 algorithm, which is used by industry but which is not a NIST-approved algorithm.
	• 128, 192, or 256-bit keys	**Y** 256 bits	WireGuard VPN uses the ChaCha20 algorithm with 256-bit keys which provides 128 bits of security.
	• Approved mode of operation per NIST SP 800-38 series	**N**	WireGuard VPN uses the ChaCha20 algorithm with Poly1305 to provide authenticated encryption per industry standards (RFC 8439); however, it does not use a NIST-approved mode of operation.
3 – Digital Signature	• DSA per NIST FIPS 186-4	**Not applicable**	WireGuard VPN protocol does not use digital signatures,
	• ECDSA len(n) >= 224		
4 – Random Bit Generation	• DRBG per SP 800-90A	**N**	Wireguard VPN software relies on the /dev/urandom and /dev/random virtual devices for random bit generation under Linux. These devices implement a ChaCha20-based cryptographic pseudorandom number generator which is not Nist-approved.
	• Hash_DRBG or HMAC_DRBG using any hash per NIST FIPS 180		

NIST SP 800-131A, Rev.2		**Compliance**	
Section – Algorithm	**Requirement(s)**	**WireGuard VPN**	**Comments**
5 – Key Agreement using Diffie-Hellman (DH)	• Diffie-Hellman per NIST SP900-56A • DH >= 112 bits of security (i.e., len(n) >= 224).	**Y** ECDH using Curve25519	WiredGuard VPN uses Curve25519, which is a NIST-recommended curve per SP800-186. The curve uses a 256-bit key that provides 128 bits of security.
6 – Key Agreement using RSA		**Note Applicable**	WireGuard VPN use Diffie-Hellman key agreement in lieu of RSA; refer to previous row.
7 – Key Wrapping		**Not Applicable**	WireGuard VPN does not use key wrapping.
8 – Deriving Additional Keys from a Crypto-graphic Key	• HMAC per FIPS 198 or • CMAC per SP 800-38B plus AES-128 per FIPS 197	**N** HMAC-BLAKE2	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function for HMAC computation. Refer to comment for "9 – Hash functions"
	• Key derivation key >= 112 bits	Y 256 bits	
9 – Hash Functions	• Secure hash algorithm per NIST FIPS 180 • SHA-224, -256, -384, -512 acceptable	**N** BLAKE2	WireGuard VPN uses the BLAKE2 algorithm as the underlying hash function. The BLAKE2 algorithm is not a NIST-approved hash algorithm; HOWEVER, it was one of the top 5 finalists out of a field of 51 entrants.for the NIST hash competition.
10 – Message Authentication Codes	• HMAC per FIPS 198; or • CMAC per SP 800-38B plus AES-128 per FIPS 197; or • GMAC per SP 800-38D plus AES-128 per FIPS 197; or • KMAC per SP 800-185 plus SHA3 per FIPS 202	**N** ChaCha20-Poly1305	WireGuard VPN uses the ChaCha20 algorithm with Poly1305 to provide authenticated encryption per industry standards (RFC 8439); however, it does not use a NIST-approved mode of operation.

Result = **PARTIAL**: This inspection shows that the industry standard algorithms used by WireGuard provide security strength and key lengths that are equivalent to the NIST-approved algorithms specified in NIST SP-800-131A, Rev. 2. HOWEVER, the underlying cryptographic algorithms themselves are not NIST-approved. Although the inspection results for SER-05 / SER-12 do not show full compliance with the MOC, other factors should be considered:

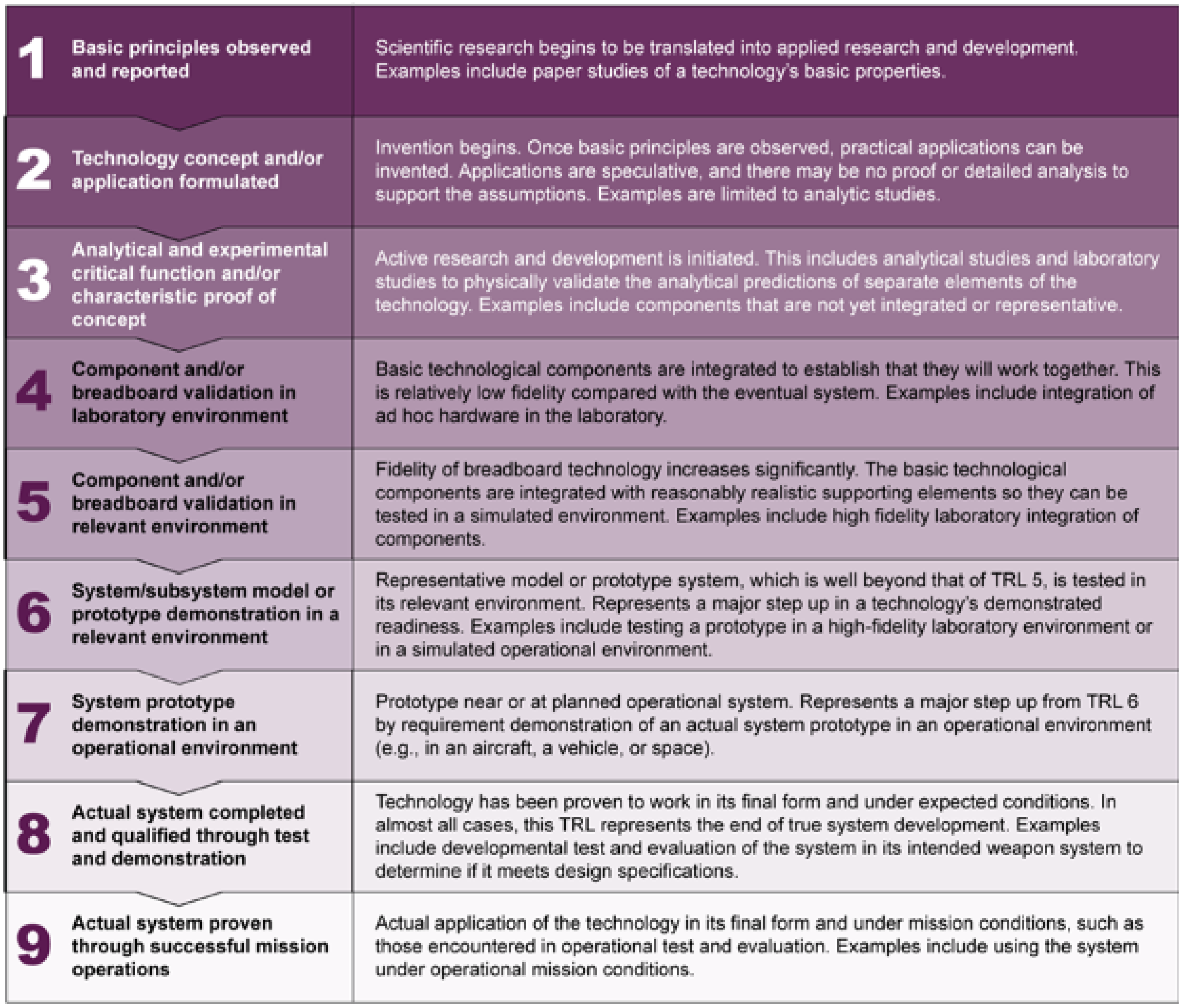
- As noted previously, WireGuard VPN has been adopted widely by commercial VPN service providers.

- WireGuard VPN has been subjected to independent cryptographic proof [INRIA], which analyzed the entire protocol and concluded that the protocol is cryptographically safe and achieves stated security goals of secrecy, forward secrecy, mutual authentication, session uniqueness, and resistance to denial of service attacks.
- Although OpenVPN and OpenSSL support NIST-approved algorithms, their code sizes are large (~400K lines of code) since they support multiple protocols (TLS, DTLS), many cipher suites (RSA-based, ECC-based), and many configuration options. By comparison, since WireGuard VPN is a focused solution, its code size is significantly (~100x) smaller, which offers a number of advantages: minimizes the attack surface, simplifies setup/configuration (i.e., less opportunity for mistakes), and improves performance (which is a key consideration for UAS C2 communications).
- The C2 Link System (DTSR-to-DTSR) security uses DTLS and a cipher suite that relies on NIST-approved algorithms, and the VPN uses the WireGuard VPN protocol and industry-standard algorithms. Together they provide two layers of security for exchanges between the UA and the CS. Having protocol and crypto-algorithm diversity mitigates the risk of both layers of security being compromised at the same time. In other words, there is still one layer of protection if the protocol/algorithms for the other layer are broken.

D. TECHNOLOGY READINESS ASSESSMENT

This section presents a qualitative technology readiness assessment of the UAS-PP system under test. The assessment leverages the nine Technology Readiness Levels (TRL) defined by the US General Accounting Office in the *Technology Readiness Assessment Guide: Bess Practices for Evaluating the Readiness of Technology for use in Acquisition Programs and Projects* (available online at https://www.gao.gov/assets/gao-20-48g.pdf). These nine levels, which are shown in the figure below, are used by US DoD, NASA, and other government organization to assess technology readiness.

Figure E-1 – Technology Readiness Levels



1	Basic principles observed and reported	Scientific research begins to be translated into applied research and development. Examples include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4	Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that they will work together. This is relatively low fidelity compared with the eventual system. Examples include integration of ad hoc hardware in the laboratory.
5	Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include high fidelity laboratory integration of components.
6	System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond that of TRL 5, is tested in its relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.
7	System prototype demonstration in an operational environment	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requirement demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, a vehicle, or space).
8	Actual system completed and qualified through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9	Actual system proven through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Source: GAO analysis of agency documents. | GAO-20-48G

The assessment of the UAS-PP system starts with the top-level systems, which include the: UA, C2 communication service providers, CS, local storage, and cloud storage. Those five systems are further divided into key sub-systems, which are then divided into constituent components that represent the technologies being assessed. The following table identifies the systems, sub-systems, and components to which a TRL is assigned using the criteria in Figure E-1. Rationale is provided to support the assessed TRL.

Table E-1 – UAS-PP Technology Readiness Assessment

System	Sub-system	Component	TRL	Rationale
UA	Drone Platform	N/A	**9**	FreeFly Alta-X is a commercial product. [Note 1]
	C2 Link System Hardware	Processor	**9**	RaspberryPi is a commercial product. [Note 1]
		Camera	**9**	ArduCam is a commercial product. [Note 1]
		SAT+5G Radios	**8**	Honeywell VersaWave avionics is a final pre-production prototype.
	C2 Link System Software	Operating System	**9**	Linux is a commercial product [Note 1]
		C2 Link System Application	**6**	Tested on an operational platform but not used for vehicle command and control
		Crypto Library	**9**	wolfSSL cryptographic library is a commercial product [Note 1]
		VPN	**9**	WireGuard VPN is a commercial product. [Note 1]
C2CSP	Cellular Communications	N/A	**9**	ATT is a commercial cellular service provider. [Note 1]
	Satellite Communications	N/A	**9**	Inmarsat is commercial Satcom service provider [Note 1]
CS	Hosting Environment	Processor	**9**	Dell laptop is a commercial computing host. [Note 1]
		Virtual Machine	**9**	VirtualBox is a commercial product [Note 1]
		Operating Systems	**9**	Windows and Linux are commercial products. [Note 1]
	C2 Link System Software	C2 Link System Application	**6**	Tested on an operational platform but not used for vehicle command and control
		Crypto Library	**9**	wolfSSL cryptographic library is a commercial product [Note 1]
		VPN	**9**	WireGuard VPN is a commercial product. [Note 1]
Local Storage	Hosting Environment	Processor	**9**	Dell laptop is a commercial computing host. [Note 1]
		Virtual Machine	**9**	VirtualBox is a commercial product [Note 1]
		Operating Systems	**9**	Windows and Linux are commercial products.
	Applications	Local Storage Management Application (LSMA)	**6**	Honeywell-developed application providing project-specific file uploading from local storage to cloud storage.
Cloud Storage	Hosting Environment	API Gateway	**9**	Kong is a commercial product
		Application Hosting	**9**	Microsoft Azure Kubernetes Service (AKS) is a commercial product. [Note 1]
	Applications	Identify Management	**9**	Single Sign On (SSO) is a commercial application that is configured by Honeywell. [Note 1]

	Data Storage and Management App (DSMA)	**7**	Honeywell-developed application providing project-specific cloud services (activity/dispatch file creation, user key pair generation, decryption of encrypted image files)
	Role-Based Access Control	**9**	Honeywell Node.js application built for accessing the RBAC database.
	Web Application	**7**	Honeywell-developed web-based user interface application (React.js application) using Honeywell’s Sentience Common UI Framework (i.e., UI design language used for production-quality Honeywell Forge programs)
Storage	File Data Storage	**9**	Microsoft Azure Blob storage is a commercial service. [Note 1]
	Dispatch Plan Database	**9**	Microsoft SQL databased is a commercial product. [Note 1]
	Role-Based Access Control	**9**	Microsoft SQL databased is a commercial product. [Note 1]

NOTES:

1. Although a final production system may select a different component and or component supplier, the component used in the UAS-PP project represents a high maturity and commercially available technology.

For the C2 Link System Application Software, the TRL level could be progressed by using the C2 link system for vehicle control instead of sending user data messages to simulate vehicle control traffic.

The LSMA would need more use cases to be considered and physical security protections to get to TRL 7. The LSMA in this projected was a VM running on a laptop; it did not have the requirements to support an actual operational environment.

The DSMA would need unit testing and additional requirements, development, and validation to get to TRL 8.

E. SYSTEM SECURITY VERIFICATION (SSV) RESULTS

Table E-1 System Security Verification Findings

Issue ID	Component	Summary	Description	Impact
74026SEC-12	Cloud Storage	Assessment: Misconfigured Sudoers File	Sudoers file is set to completely open allowing anyone to use sudo with no security challenge.	A configured Sudoers file allows anyone on the system to act as root with no security challenge
74026SEC-11	Cloud Storage	Assessment: Poor Password Management	Password management is mostly non-existent.	Lack of password policy allows users to have short unsecure passwords that never change, among other things, which can slowly lead to a higher chance of one of those passwords being compromised
74026SEC-10	Cloud Storage	Assessment: CUPS Service	CUPS service is old and popping as vulnerable.	Older versions of services are often vulnerable to previously discovered flaws, recommend simply upgrading to a newer version or removing entirely
74026SEC-9	Cloud Storage	Assessment: Poor Password Management	Passwords do not expire.	Passwords should be rotated and properly managed to ensure possible vulnerabilities due to passwords is reduced.
74026SEC-8	Cloud Storage	Assessment: Linux Sudoers Priv Esc	Sudoers file has had all the security settings turned off.	A misconfigured sudoers file makes priv esc easier for attackers who manage to get control of a basic account. They can simply run sudo to execute commands as root, with no challenge.
74026SEC-1	Cloud Storage	Assessment: Cache-Control Header Missing	Cache-control header is missing in the responses from the application.	Sensitive data could be cached in a client's browser, and accessed by another use on the same device.

74026SEC-2	Cloud Storage	Assessment: HTTP Methods Enabled	PATCH and PUT methods are enabled.	Unnecessary HTTP methods can add additional attack surface.
74026SEC-3	Cloud Storage	Assessment: Rate Limiting	There does not seem to be a limit to the amount of requests that can be sent to the application.	Without rate limiting an attacker could create a denial of service situation against the application.
74026SEC-4	Cloud Storage	Assessment: Unrestricted File Upload	The application does not check to see what sort of file the user is uploading.	Unrestricted upload could allow an attacker to upload malicious content. If the application or a backend admin allowed malicious content to execute, there could be a serious compromise.
74026SEC-5	Cloud Storage	Assessment: XSS Header Not Secure	The 'x-xss-protection' header is present but does not seem to be configured.	Not using good cross site scripting defense and proper settings can increase the possibility of a cross site scripting attack being successful.
74026SEC-6	Cloud Storage	Assessment: Input Validation	The application seems to accept just about any character and any number of them in the event creation inputs.	Lack of input validation allows an attacker to enter malicious content or deface the application.
74026SEC-13	UAS	Open Source Vulnerabilities in UAS	The current version of the UAS is affected by multiple open source vulnerabilities.	The current version of the UAS is affected by multiple open source vulnerabilities.
74026SEC-14	Control Station	Open Source Vulnerabilities in CS	The current version of the CS is affected by multiple open source vulnerabilities.	The current version of the CS is affected by multiple open source vulnerabilities.
74026SEC-15	LSMA	Open Source Vulnerabilities in LSMA	The current version of the LSMA is affected by multiple open source vulnerabilities.	The current version of the LSMA is affected by multiple open source vulnerabilities.

74026SEC-16	UAS	Mission Data Unencrypted at Rest in UAS	Mission data appears to be unencrypted at rest, but it is encrypted in transit back to the CS.	Confidentiality and integrity compromised. Business impact also considered due to proprietary nature of the information.

This page intentionally left blank.