



Fires' Cell Transition to SBU-E

(SBU-E AFATDS Set-up and Protocol)

**NO.25-999
May 2025**

Disclaimer: CALL presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Authors are responsible for the accuracy and source documentation of material they provide.

Authors: 1LT Blazek, Quinn and SFC Cundiff 2MBCT, 101st Airborne (Air Assault)

Introduction: Validating the SBU-E Kill Chain

During Operation Lethal Eagle (OLE) 4, 2nd Brigade Combat Team (BCT) “Strike” successfully validated the new Sensitive but Unclassified-Encrypted (SBU-E) kill chain, extending digital communications from the Battalion Fire Support Element (BN FSE) via Mobile User Objective System (MUOS) to the Brigade (BDE) Advanced Field Artillery Tactical Data System (AFATDS) to Division (DIV) Fires (using a Secret Internet Protocol Router (SIPR) network) 1-320th Field Artillery Regiment Fire Direction Centers (FDCs), and ultimately to the artillery guns. This report outlines the difficulties, successes, and unresolved issues the BDE Fires Cell encountered during OLE 4. In the appendices following the report show the reader “a way” to set up this equipment for operation.

Initial Setup & MCP Configuration

During OLE 4, 2nd BDE tested a new Mobile Brigade Combat Team (MBCT) Main Command Post (MCP) concept, designed to create a lighter and faster Current Operations (CUOPS) section. While showing promise, this new setup presented logistical challenges, primarily related to integrating the SBU-E network, Integrated Tactical Network equipment, and the new MCP configuration. This configuration included a dedicated “antenna farm” – two radios (MUOS-Voice and MUOS-Digital) positioned away from the MCP to minimize electromagnetic (EM) interference.

Network Integration Challenges

Setting up the new MCP presented integration hurdles. The S6 section resolved numerous network routing issues specific to the new concept and the SBU-E network. Troubleshooting the radio connection proved more complex due to the distance between the MCP and the antenna farm. Another unique challenge for the S6 as MUOS point-to-net (PTN) configurations are specialized for field artillery digital communications. A Soldier from the S6 section had to monitor radio traffic at the antenna farm, and direct communication via an alternate network (Tactical Scalable Mobile Ad-hoc (TSM)) proved vital for troubleshooting, particularly when the MUOS radio experienced outages or PTN drops due to heat.

EM Mitigation and Radio Configuration

To mitigate EM emissions, the two mounted 158 radios in the Fires’ vehicle remained powered off when static. The digital radio at the antenna farm mirrored the vehicle’s digital radio profile to maintain consistent IP addresses for digital communications. As detailed in the appendices, configuring digital MUOS is intricate, and the distance between CUOPS and the antenna farm amplified these complexities.

Power and Infrastructure Limitations

The BDE Fires Element relied entirely on the S6 section for communication support, as all communications flowed through their network. However, the vehicle’s intended power source, an inverter, proved unreliable due to exhaust fumes and noise, forcing CUOPs vehicles to draw power from the MCP generator. This created a single point of failure. Later, a generator malfunction disrupted all communications, including Mounted Mission Command (MMC), NIPR,

AFATDS, and voice communication (NMP running Instant Connect Enterprise (ICE)). Reconfiguring the systems during MCP movements required Soldiers to physically disconnect and reconnect network cables, demanding careful organization and cable management.

Throughout the exercise, we encountered various standard technical issues. Radios required frequent re-fills. Radios that would get stuck in the initializing and configuring process that ultimately required us to reload the AFATDS software after two days of testing and ruling out every possible physical connection, radio connection, or network issue.

Key Requirements and Recommendations

- The BDE S6 section needs to carry extra encryption keys to ensure access to critical equipment.
- The S6 section needs the ability to load Fires' radios, as the Fires team owns the MUOS Fires network.

Interoperability & PACE Plan Limitations

After working through these technical issues, the Primary, Alternate, Contingency, and Emergency (PACE) plan to the Division was difficult to execute. Because Division only carries classified systems; For our SBU-E AFATDS, we could still talk to DIV. But if SBU-E Upper Ti went down, there was no alternative beyond NIPR communications over Microsoft Teams or cMMC (both of which would frequently go down simultaneously). The only solution when NIPR lost connection was to use a MiFi puck for connectivity. However, the MiFi puck's Wi-Fi signal directly contradicts the intent to reduce EM emissions in the MCP.

SBU-E Network Functionality & Architecture

The SBU-E network presented an initial learning curve but once mastered, Fires maintained digital communications throughout the operation. This learning curve stemmed from the complex interactions between SBU-E and other systems. At the lowest level, SBU-E utilizes the Tactical Radio Integration Kit (TRIK). Communication between systems relies on the Network Address Translation (NAT) IP, rather than the systems' native IP. Higher level traffic passes through a Tactical Cross Domain Solution (TACDS) which de-NATs/de-PATs and re-NATs/re-PATs the traffic. However, the TACDS does not support AFATDS Data Protocol (ADP), requiring workarounds for data exchange. To enable communication between systems, the unit configured the system name as "VMF 6017C System" and System Type "47001C/VMF 6017C" in their MUL entry. AFATDS can send limited VMF (6017C) messages. (Appendix C for details). Currently, manual data transfer ("swivel chair") is required between the SBU-E Tactical Airspace Integration System (TAIS) and the classified TAIS due to incompatibility.

Communication Successes & Identified Issues

SBU-E communication between Fire Supporters, FDCs and the unclassified TAIS and the BDE Fires CUOPs box functioned successfully. However, we identified issues when transmitting data from SIPR to unclassified systems, including instances of point targets converting to circular targets. DIVARTY has published a white paper addressing these issues. Detailed configuration instructions for SBU-E Upper Tier and MUOS (D) are included in the appendices, these enabled the BCT to maintain lethal digital communications.

Conclusion & Future Implications

In conclusion, SBU-E enhances interoperability between echelons and fosters collaboration on the battlefield. The initial learning period associated with the new methodology allowed operators to identify areas for improvement and develop preliminary procedures. Through these challenges, the team gained a deeper understanding of hardware, software, waveforms, and network capabilities. The Brigade level kill chain, from shooter to sensor, now leverages unclassified technology without compromising coordination with the Division's classified systems.

Appendix A - A way to set up SBU-E LAN via Upper Ti

Appendix B - A way to set up your boxes via MUOS (D) Unclassified

Appendix C - Sample of ADP -> VMF Messages That Will or Will Not Transmit

Appendix D - A Way to Add a Static Route Via Command Prompt

Appendix A

A way to set up SBU-E LAN via Upper Ti

To set up **SBU-E LAN via Upper Ti**, plug in the ethernet cable into the primary LAN port. In IPV4 advanced settings, build:

-IP Address is issued by S6.

-Subnet Mask is subject to change: (i.e. 255.255.255.224)

-Gateway is: -5 of the IP. (i.e. 10.64.51.166 -> 10.64.51.161)

-Preferred DNS server should match Default Gateway

In the Communication Workspace, build another primary LAN. Do NOT use the automated primary LAN designated by the Communication Workspace in the AFATDS software (keep it inactivated). To do so, in the Communication Workspace, click on current -> New -> IP -> Ethernet -> enter in all IPV4 information.

NOTE: For the local unclassified TAIS, confirm the System Name is "Tais" and System Type is "47001C/USMTF 04" in the MUL entry.

Appendix B

A way to set up your boxes via MUOS (D) Unclassified

Here's how the BN FSE and BDE FSE communicate via MUOS-D unclassified, assuming Soldiers loaded correctly all necessary encryption keys and mission plans.

The following section will outline the MUOS setup process:

-5 Zero -> Activate Mission Plan to

Bootstrap the radio:

-3 Mode -> Maintenance -> Harris1680 (password) -> Enable Maintenance mode.

-Power Cycle the Radio-

-7 Options -> Channel 1 -> MUOS Config -> Settings -> User Profile (Delete) -> Create Bootstrap (Yes). The bootstrap will take approximately 20 minutes.

Once MUOS has configured (CFG), initialized (INIT), and found the satellite and become operational "OPER",

-8 Program:

-> System Presets -> Preset Config -> Select MUOS Channel (back to initial 8 Program screen)

-> Advanced -> Static (everything) (back to initial 8 Program screen)

-> IP data -> (change streaming) File Transfer -> QOS bit rate 9600 -> Max bit rate 32000

Close 8 program

-7 Option -> Channel 1 -> Network Options -> Interfaces -> Red interface -> Ethernet

-7 -> Option 1 -> Channel 1-> Radio Options -> Radio Silence off -> Handset Lapel Mic-> AUX power 8 volts -> AUX data on -> Preset autosave on -> RF faults persists on -> PA failure override disabled -> Suppress VSWR faults

-1 -> Activate Service -> IP Network (should say PTN in bottom left; GRP directly above PTN)

Make sure to get the angle of the directional antenna to the satellite from your S6 and check that the connection strength is below -118.

To pull your MUOS IP Address, go:

-7 Options -> Channel 1 -> Network Options -> Red Interfaces -> Ethernet -> Primary IP

In the AFATDS, plug the MUOS LAN Cable into the AFATDS secondary LAN port. Configure a secondary LAN in IPV4 advanced settings in Ethernet 2 port as such:

-IP Address is: +2 of the AN/PRC-158's Radio IP (i.e. 10.194.76.97 (Radio) -> 10.194.76.99 (AFATDS))

-The subnet mask will change depending on mission plan: (i.e. 255.255.255.248)

-The default gateway, preferred DNS server, and alternate server is **BLANK**. On SBU-E, there cannot be 2 default gateways like you would with a SIPR box. (**Appendix D** is a way to add a

static route via command prompt but there is another way that I will explain further down.)

In the Communication Workspace, build a secondary LAN for the MUOS LAN. To do so, click on current -> New -> IP -> Ethernet ->

- Network Name: MUOS

- Network Hostname: MUOSDIG

- Local IP Address: +2 of radio (AFATDS IP)

- Subnet mask: Same as built in IPV4 settings

Click “OK” to create network. Under networks, double click MUOS to open it. Unplug the MUOS ethernet cable from the back of the AFATDS. Type in the actual radio IP into “Router IP Address” located at the bottom of the pop-up window. (If you leave the MUOS ethernet cable plugged in, it will grey out the router IP address and not allow you to enter). Click “OK”. Plug the MUOS ethernet cable back in. This is another way to create a static route as mentioned previously.

Click “Communication Device” tab and under “Assigned Network” assign MUOS to secondary LAN. Then, back in “Network Data” turn on the route.

MUOS can take a long time to send data. In Command Prompt, pinging a destination host’s IP can sometimes time out because the AFATDS expects an immediate response. This does not necessarily mean that digital communications will not work—send a free text to verify and it will sometimes build the route, turning the route green in Communication Workspace. When initializing, send a test message using the “Open Network Diagram” button.

Appendix C

Sample of ADP -> VMF Messages That Will or Will Not Transmit

				Intervention point was grayed out. NO MET CM Data
	Cancel Check Fire by Fire Plan	Not Tested	Not Tested	
	MET CM	Not Tested	Not Tested	NO MET CM Data
	Friendly Unit Data	Yes/yes	No/No	Unit information is being purged does not work in VMF
	Enemy Unit Data	Yes/yes	No/No	pushing enemy non AFATDS units is not supported VMF
	MIDB Facilities, Units, JDPI, HVI, POI and Equipment	Not Tested		NO MIDB
	MIDB RTL	Not Tested		NO MIDB
	MIDB NSL	Not Tested		NO MIDB
	Tracks	Not Tested	Not Tested	No Simulation
K2.08	Named Target List	Yes/yes	Yes/Yes	
	Planned Target List	yes/yes	Yes/yes	
K2.09	Counter Fire Target List	Yes/Yes	Yes/Yes	Received VMF message- input graphic display, did not create counter fire target list
	NCTL	Yes/Yes	no/no	Sends target list but not as collaborative list
	ASL	Yes/Yes	No/No	Did not receive on VMF. Was failing on AFATDS control box. Received on ADP system.
	Target Info Query	Not Tested	Not Tested	
K2.04	Immediate Air	Yes/Yes	Yes/Yes	
	REQSTATASK	Not Tested	Not Tested	
	MISREP			
	Preplanned ASR	Yes/Yes	No/No	Did not receive ASR on VMF, had to send as a fire mission to the ADP.
K2.15	Transfer Current	Yes/No	Yes/Yes	Current was not received on ADP system, was volatile would send graphical but no data.
	Transfer Plan			
K02.48C	Guidance			
	UXO Spot Report			
	UXO Mission Report			
	Geometries	yes/yes	yes/yes	

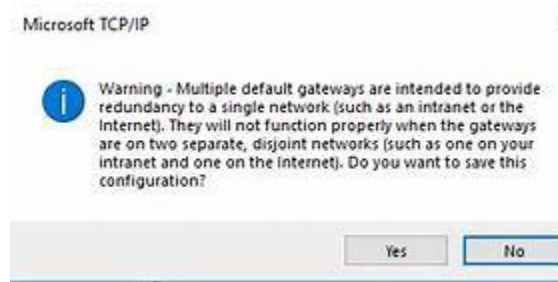
				Intervention point was grayed out.
	Cancel Check Fire by Fire Plan	Not Tested	Not Tested	NO MET CM Data
	MET CM	Not Tested	Not Tested	NO MET CM Data
	Friendly Unit Data	Yes/yes	No/No	Unit information is being purged does not work in VMF
	Enemy Unit Data	Yes/yes	No/No	pushing enemy non AFATDS units is not supported VMF
	MIDB Facilities, Units, JDPI, HVI, POI and Equipment	Not Tested		NO MIDB
	MIDB RTL	Not Tested		NO MIDB
	MIDB NSL	Not Tested		NO MIDB
	Tracks	Not Tested	Not Tested	No Simulation
K2.08	Named Target List	Yes/yes	Yes/Yes	
	Planned Target List	yes/yes	Yes/yes	
K2.09	Counter Fire Target List	Yes/Yes	Yes/Yes	Received VMF message- input graphic display, did not create counter fire target list
	NCTL	Yes/Yes	no/no	Sends target list but not as collaborative list
	ASL	Yes/Yes	No/No	Did not receive on VMF. Was failing on AFATDS control box. Received on ADP system.
	Target Info Query	Not Tested	Not Tested	
K2.04	Immediate Air	Yes/Yes	Yes/Yes	
	REQSTATASK	Not Tested	Not Tested	
	MISREP			
	Preplanned ASR	Yes/Yes	No/No	Did not receive ASR on VMF, had to send as a fire mission to the ADP.
K2.15	Transfer Current	Yes/No	Yes/Yes	Current was not received on ADP system, was volatile would send graphical but no data.
	Transfer Plan			
K02.48C	Guidance			
	UXO Spot Report			
	UXO Mission Report			
	Geometries	yes/yes	yes/yes	

	CGRS		
	CGRS Nominations		
K02.10C	Fire Plan		
K02.8C	Schedule of Fires		
?	Groups		
?	Series		
K02.7C	Survey Control Points		
K03.2C	ENGAGE RPT/BDA		
K02.15C	FIRE SUPPORT COORDINATION MEASURES	YES/YES	Yes/Yes
K02.10C	FIRE PLAN MISSION / FIRE PLAN CANCELLATION		
K1.01	Mission Takeover		

Appendix D

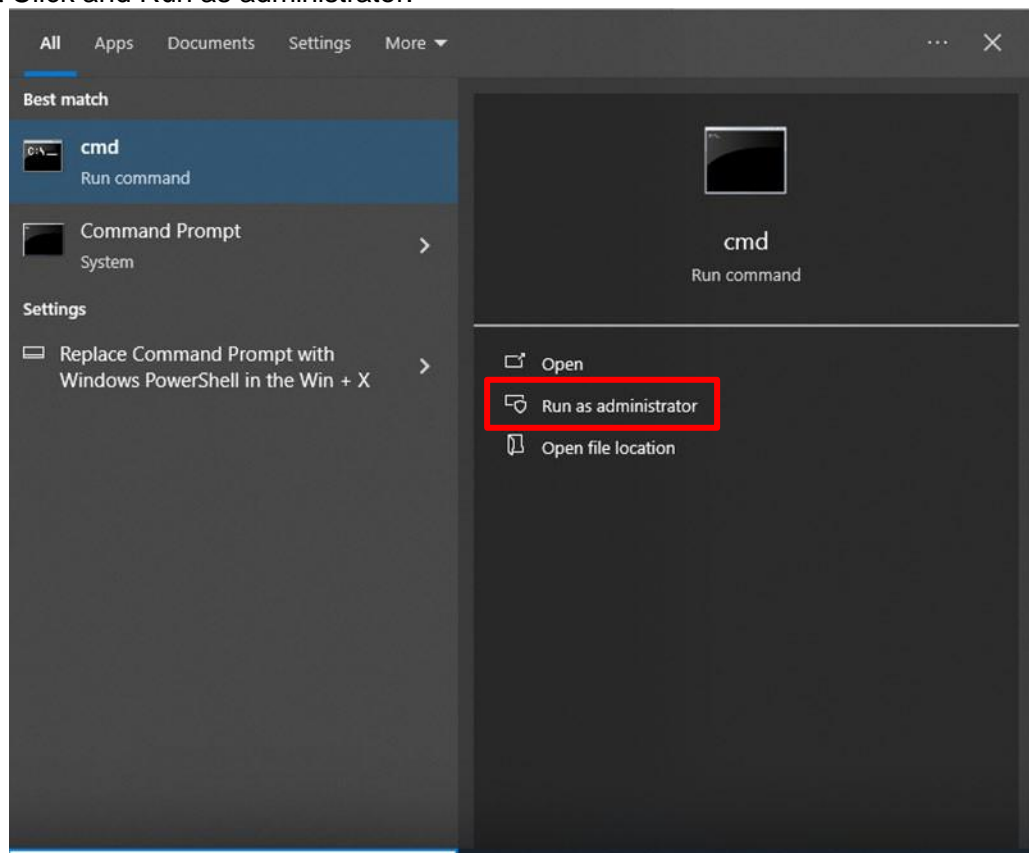
A Way to Add a Static Route Via Command Prompt

Issue: MUOS at the BDE (UNCLASS) Reported to have issues, the only connected network the AFATDS was on was MUOS, and not SBU. They were experiencing issues when connected to both, and the following error pops up when the AFATDS is connected to different networks, with two default gateways.



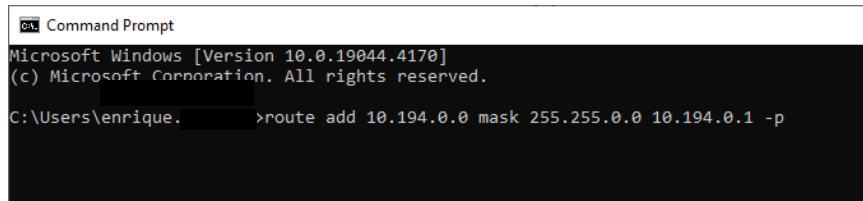
Action:

1. Removed the default gateway on the MUOS interface and added a static route for the entire MUOS Network pointing to the MUOS Radio.
2. The following procedure was done to install MUOS persistent route.
 - a. Start>Command Prompt
 - b. Right Click and Run as administrator.



- c.
- d. Acknowledge the pop up for administrative privileges.
- e. Add the persistent static route (-p makes it persistent so it does not get removed upon a reboot of the AFATDS box)

3. Type the following command, in command prompt.
 - a. Route add 10.194.0.0 mask 255.255.0.0 <MUOS RADIO IP> -p



```
Command Prompt
Microsoft Windows [Version 10.0.19044.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\enrique.>route add 10.194.0.0 mask 255.255.0.0 10.194.0.1 -p
```

- b.
- Keynote: 10.194.0.1 is an example for the MUOS Radio IP**
- c. Command Prompt provides an “OK!” to inform the user of success.
4. Verify AFATDS routing table.
 - a. Type the following command, in command prompt and Check the Persistent Routes
 - i. Route print
 - ii. 0.0.0.0 0.0.0.0 should be pointing to the SBU-E 10.64.X.X server default gateway.
 - iii. 10.194.0.0 255.255.0.0 should be pointing to the MUOS 10.194.X.X Radio IP
5. In the Comms Workspace **Activate** Primary LAN (SBU-E) Network prior to the MUOS Network

Result: BDE FUOPS and CUOPS reported two-way communication on both MUOS and SBU-E while simultaneously connected.

