COLUMBIA SCIENTIFIC BALLOON FACILITY

CSBF FLIGHT SYSTEM AND GROUND SUPPORT EQUIPMENT NETWORK HANDBOOK

ES-100-00-H
REV. A
RELEASE DATE: APRIL 07, 2026

COLUMBIA SCIENTIFIC BALLOON FACILITY
PALESTINE, TEXAS 75803

NATIONAL AERONAUTICS AND
SPACE ADMINISTRATION

This page intentionally left blank.

APPROVALS

Scott Miller (affiliate) Digitally signed by Scott Miller (affiliate)
Date: 2026.04.07 14:49:53 -05'00'

Scott Miller
Electrical Engineering
Columbia Scientific Balloon Facility
Peraton Inc.

Date

TABLE OF CONTENTS

1 INTRODUCTION AND PURPOSE

This guidance document is an introduction to the computer networks used at the Columbia Scientific Balloon Facility, field locations, and onboard scientific balloon gondolas. The guide is intended to give science principal investigators and their teams enough information to start planning, discussing, and implementing their Ethernet network architectures, including flight equipment and GSE interfaces with CSBF equipment and facilities.

Note that this guide is specifically geared towards computer networking interfaces for flight systems and GSE and leaves out information on non-network based or legacy electrical interfaces used on both Conventional and LDB missions. See the Resources section for links to information on those interfaces.

2 DEFINITIONS/ACRONYMS

ANT	Antarctica
ASC	Antarctic Support Contract
BPO	Balloon Program Office
CGNAT	Carrier-Grade Network Address Translation
CIP	Consolidated Instrument Package
CSBF	Columbia Scientific Balloon Facility
EVTM	Ethernet Via Telemetry
FTS	Ft. Sumner, New Mexico
GSE	Ground Support Equipment
HGA	High Gain Antenna
IKEv2	Internet Key Exchange Version 2
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
Kbps	Kilobit-per-second
LCT2	Low-cost TDRSS Transceiver
LDB	Long Duration Balloon
LOS	Line of Sight
Mbps	Megabit-per-second
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NSF	National Science Foundation
OCC	Operations Control Center
OTH	Over the Horizon
SIP	Support Instrumentation Package
SSH	Secure Shell / Secure Socket Shell
TCP/IP	Transmission Control Protocol / Internet Protocol
TDRSS	Tracking and Data Relay Satellite System
UDP	User Datagram Protocol
VPN	Virtual Private Network

3 GETTING STARTED, SUPPORT, AND RESOURCES

3.1 GETTING STARTED

The best way to get started working with the computer networks at CSBF is to understand what network resources will be available during your mission and how these resources can be used to support your science objectives. Each mission type, launch location, and gondola communications combination will present a unique network environment.

CSBF recommends early collaboration on your specific communications and network needs with the CSBF staff assigned to your mission. Use the Support resources below to reach out when ready to begin having technical interchanges.

3.2 SUPPORT

Balloon Program Office

Contacts: https://www.nasa.gov/scientificballoons/mediaresources/

For initial contact with the NASA Balloon Program Office regarding your mission, reach out to the NASA Mission Operations Manager at the NASA BPO. A mission manager will be your main NASA point of contact throughout the mission timeline. They will route your question to the operations staff assigned to your specific mission as needed.

Columbia Scientific Balloon Facility

The team at CSBF will be directly involved in the integration of balloon systems with your science instrument and all pre-flight, flight, and post-flight operations support.

Each balloon mission will be assigned to a Campaign Manager at CSBF. The CSBF Campaign Manager is the main point of contact for operations and logistics support throughout the campaign timeline. There will also be a Payload Engineer assigned to the campaign, which is your main point of contact for all electrical interfaces.

3.3 RESOURCES

CSBF "Fly with Us" Support Document Library

Located at: https://www.nasa.gov/scientificballoons/flywithusdocuments/

A collection of guidance documents and best practices published by CSBF to support science. For non-network based electrical interfaces, see the "Conventional Balloons Operations Support" and "Long Duration Balloon Support for Science" documents. These will introduce current and legacy electrical interfaces with CSBF equipment.

Scientific Ballooning Handbook 50th Anniversary Edition

Located at: https://ntrs.nasa.gov/citations/20240004989

A recently updated (2025) handbook discussing all facets of scientific ballooning, including common approaches to telemetry & data recovery, command & control, satellite communications including Starlink, and various considerations and recommendations in each section.

4 General Computer Network Information

General use internet capabilities at CSBF and field locations

All CSBF facilities have wired and wireless general use internet available.

In Antarctica, CSBF WI-FI (provided via Starlink) as well as NSF/ASC WI-FI access are available at the LDB facility. NSF/ASC WI-FI and wired internet access are also available at McMurdo Station in select locations. Note that NSF/ASC WI-FI is highly restrictive and subject to a formal request process starting early in the mission planning stage. Discuss your needs with the CSBF Campaign Manager and CSBF IT Support to see if NSF/ASC internet access will be beneficial to your mission.

Ground Support Equipment requiring a network connection

You should plan for a GSE network connection if any of the following apply:

- Your GSE requires outbound internet access (for relaying data, reverse tunnel for remote command and control, etc.).
  - The stateful network firewall will generally allow all outbound traffic initiated at the local GSE with a destination outside the local network (any destination on the routable public internet).
  - In Antarctica, CSBF internet is provided by Starlink. Be aware that the Starlink network blocks certain protocol/port combinations upstream of CSBF, which CSBF does not control. See this link or search "what ports does Starlink block" for more information. ISPs for other CSBF locations may have similar restrictions; discuss your needs with CSBF IT Support to confirm support.
- Your GSE requires inbound internet access (for remote connection to the local GSE when not using a reverse tunnel, for example).
  - Note this requires early coordination with CSBF IT Support to discuss your requirements, options for support, and any restrictions.
- You plan to receive Quasonix EVTM data packets from the gondola at your GSE. Note that LOS EVTM data is only accessible by GSE located in the field during flight operations, and OTH TDRSS EVTM data is only accessible by GSE located in the Palestine OCC during LDB flight operations.
- You plan to receive data using the CSBF Starlink VPN solution at your GSE.

Gondola telemetry links requiring a network connection

Using the following telemetry links will require an Ethernet network connection with your flight equipment:

- SpaceX Starlink
- Iridium Openport
- Quasonix EVTM:
  - LOS EVTM
  - OTH TDRSS EVTM

Physical interfacing for flight systems or GSE network connections

For CSBF provided or managed network interfaces, connections are made using RJ45 Ethernet jacks and Ethernet patch cables unless special accommodation is requested. Science teams should bring sufficient Ethernet cables for their flight and GSE connections. Consider the expected flight environment (near vacuum, temperature swings, UV radiation) when evaluating Ethernet cable suitability for flight.

Most CSBF flight equipment auto negotiates a full duplex 10/100Mbps Ethernet connection. If you have a specific need for half/full duplex or 10/100/1000Mbps Ethernet connection to your device, discuss your needs with the CSBF Payload Engineer during mission planning.

CSBF plans for 1 physical Ethernet connection from the science flight equipment on the gondola. If you require additional physical ports, consider consolidating your ports on an Ethernet switch upstream, or discuss with the CSBF Payload Engineer during mission planning (i.e., well before arriving at the CSBF/field location) to see if additional switch ports are available.

For flight systems intended to be electrically isolated (most LDB missions) you must ensure the Ethernet cable used to connect with CSBF equipment does not pass its shield through the RJ45 connector. This *will* cause electrical compatibility issues and loss of electrical isolation if not addressed.

5 Ethernet-based Telemetry Specific Information

5.1 SpaceX Starlink

Starlink provides an internet connected Ethernet interface with data throughput higher than other satellite-based links used on balloon missions. See the Scientific Ballooning Handbook link in the resources section for performance examples on past flights. It is important to note that CSBF has no direct control over the SpaceX Starlink constellation or RF link.

When planning your Starlink telemetry architecture, it is recommended to utilize unicast with UDP as your transport protocol. TCP/IP will be less performant over satellite links due to how the transport protocol handles satellite-based links like SpaceX Starlink.

In 2026, CSBF will be studying the effects of gondola rotation on Starlink Mini and Starlink Performance antenna hardware in addition to the reported synchronized reconfiguration that occurs every 15 seconds across the Starlink constellation. On some balloon missions, a correlation between gondola rotation and reduced Starlink connectivity has been observed. The results of this testing and any actionable advice will be added to a future revision of this guide.

There are two options for Starlink network support, science team managed, and CSBF managed:

Science Managed

CSBF provides Starlink hardware, service, and powers the hardware, but the science team handles all other aspects of the interface to Starlink (physical mounting and flight network architecture). The Starlink terminal is operated in Bypass Mode with no Starlink router.

This option gives the science team full control over how the Starlink gondola network is implemented. Starlink can be configured with a CGNAT'd public IPv4 IP, or a non-CGNAT'd public IPv4 IP at science request. Be aware that not using CGNAT implies the Starlink terminal provides no inbound firewall; incoming traffic from the public internet is allowed. Plan your security posture accordingly.

Neither option provides at static IPv4 IP address; depending on flight location and gondola movement the public IP of the Starlink terminal may change several times during flight.

CSBF Managed

CSBF provides the Starlink hardware, service, manages the physical mounting, powers the hardware, and manages the flight network architecture. An RJ45 Ethernet port and network configuration details are provided by CSBF to science for interfacing with the system. The Starlink terminal is operated in Bypass Mode with no Starlink router, with an industrial router upstream of the science interface.

Like in the science-managed case, the public IPv4 IP address of the gondola Starlink terminal is dynamic and may change during the mission. CSBF can provide a dynamic DNS hostname for the gondola terminal. When the public IPv4 IP changes, the hostname typically updates within 3 minutes (provider-dependent; e.g., Google/Cloudflare resolvers).

This option simplifies the gondola network implementation for the science team. CSBF will provide a VPN connection from the gondola network to the GSE mission network. The science flight equipment can use this connection to communicate directly with their GSE computer using the VPN, and the flight equipment can still send data to any other routable destination on the internet (such as a GSE at their home institution). In summary, outbound traffic from the gondola can be routed either to the wider routable public internet, or routed to the GSE mission network, based completely on the destination network address of the communication.

CSBF places a stateful firewall between the gondola network and the Starlink terminal. All gondola outbound traffic is allowed, however, Starlink blocks certain ports/protocols upstream, outside of CSBF control. All unsolicited gondola inbound traffic is blocked by default. If your mission requires inbound communication to the gondola, there are 3 general ways to accomplish this:

- Use the CSBF gondola-to-mission-network VPN
    - The gondola network devices can directly access the GSE mission network devices and vice versa using the CSBF VPN connection. Gondola or GSE devices can communicate via routed IP connectivity as if they were on connected private networks (note broadcast/multicast do not traverse the VPN).
- Directly communicate with the gondola using the Starlink public IP address
    - Coordinate with the CSBF Payload Engineer to set up the required firewall passthrough. These connections will be limited to a specific source IP range (your home institution's public IP or range of IPs, as an example), a specific internal network IP (your science flight equipment local network IP), and which network port your flight equipment is listening to (for example TCP port 22 for SSH). Keep in mind the public IPv4 address is dynamic as previously described; ensure your GSE software has a way to change destination IP when using this method.
- Implement a reverse tunnel of your own
    - There are many ways to implement this. As outbound connections are always allowed by default, the science flight equipment can tunnel out to a remote host, then use that tunnel for communications from the remote host to the flight equipment. Keep in mind the gondola public IP will be dynamic when planning your remote host/home institution firewall rules.

See the Mission Network Configuration sections for network architecture details.

5.2 IRIDIUM OPENPORT / PILOT

Note: Iridium Openport is the satellite service network, while Iridium Pilot is the hardware terminal. The Iridium Pilot hardware went end-of-life in 2019, however the Iridium Openport service remains available for the time being. CSBF's remaining inventory of terminals have all flown and been refurbished. Consequently, Iridium Pilot can no longer be used for mission critical applications, and remaining flight-worthy hardware is in short supply at CSBF.

Iridium Pilot provides an internet connected Ethernet interface to the gondola network. Data transmission with TCP/IP and/or UDP can traverse this link to the routable public internet. This is a higher latency service, and default TCP/IP timeouts have been shown to have problems. For this reason, UDP applications are highly encouraged. The throughput may burst up to 128Kbps, however average performance is between 80 and 100Kbps.

Data originating from the gondola (return TM) are sent through the Pilot access point in the same manner as a standard internet connection. Data sent to the gondola (commands / forward TM) must address the Pilot's static external IPv4 IP address at a specific pre-arranged port number, and the source IPv4 IP address of the communication must be added to the service provider's firewall. Port forwarding rules then route data to the corresponding internal IP address and internal port based on the external port of inbound communication. Work with your CSBF Payload Engineer early in mission planning if you use this option to set up the required configuration.

If you plan to use multiple internet gateways on a balloon mission (such as SpaceX Starlink and Iridium Openport), each internet gateway will be on a different network subnet on the gondola (even if connected to the same physical Ethernet switch). Your flight hardware must either provide a physical Ethernet interface to each internet gateway or be capable of selecting or prioritizing between multiple network subnets/gateways in software with a single physical Ethernet connection.

5.3 QUASONIX EVTM – LOS & TDRSS OTH

Note: TDRSS EVTM requires specific CSBF hardware for support. The LCT2 hardware is required as a base for OTH EVTM, and data rates above 10Kbps require a TDRSS HGA. CSBF has a limited supply of both LCT2 and HGA hardware available, and the HGA specifically cannot be used for mission critical purposes as the units have all flown multiple times.

The Quasonix EVTM provides a unidirectional Ethernet link from the gondola to a mission network either at the launch location (in the case of LOS EVTM) or at the Palestine, TX OCC (in the case of TDRSS OTH EVTM). LOS EVTM can be used on conventional or LDB missions, while TDRSS OTH EVTM is only available on LDB missions. An LDB mission may have both interfaces present.

Ethernet frames entering the EVTM encoder interface on the gondola network are output from the EVTM decoder interface on the GSE network unmodified. A network switch is used to connect science flight equipment or GSE to the EVTM interface(s). A 16Mbit buffer is used by the EVTM encoder, with the buffer drain clocked by the RF link clock. Overrunning the buffer will result in data loss.

LOS throughput is up to 16Mbps and TDRSS OTH throughput is 300Kbps or more depending on satellite availability. Note there is a combined TDRSS throughput limit across all missions of 1.4Mbps into CSBF's network. Available TDRSS scheduling windows, and window duration, decrease as throughput increases beyond 300Kbps.The EVTM throughput figures are total link throughput; be sure to account for Ethernet framing overhead when calculating maximum data rate. Quasonix recommends the data throughput not exceed 90% of the link throughput for this reason.

As the EVTM link is unidirectional, UDP broadcast and multicast must be used to transmit data across the link. UDP multicasting is preferred to broadcasting as broadcasts must be received and processed by all devices on the network subnet, which can lead to network congestion. In the case of TDRSS OTH EVTM used in conjunction with LOS EVTM on the same mission, the use of multicasting is required by CSBF as interface selection is determined by multicast group destination using multicast filtering at the network switch level. The CSBF Payload Engineer can discuss these options with you and provide specific guidance on multicast group or broadcast IPv4 IP addresses to use.

6 CONVENTIONAL MISSION NETWORK CONFIGURATION

GSE Network

The mission network located at the conventional mission field location is used for all science GSE, and network access for devices like printers. Critical GSE are typically given static IPv4 IP address reservations based on their hardware MAC addresses. Other devices use DHCP IPv4 IP address assignment. CSBF IT Support manages all aspects of the field mission network, with collaboration from the CSBF Payload Engineer.

Devices on the mission network will have outbound internet access by default. If remote access to GSE is requested, CSBF IT Support can provide two options: SonicWall NetExtender VPN (preferred), or NAT translation/port forwarding firewall rules. The SonicWall NexExtender VPN requires that the remote client can run the NetExtender VPN client. The NAT translation option maps a CSBF public IPv4 IP address and port combination to the GSE's private IPv4 address and port and allows this access to a defined set of remote public IPv4 IP addresses/ranges of addresses only (typically a home institution).

LOS EVTM telemetry will be returned to the field mission network. As mentioned in the general EVTM section, UDP multicast (preferred) or UDP broadcast are used to traverse the EVTM link from gondola to GSE networks. If using UDP broadcasting, the GSE equipment subnet mask must overlap with the IPv4 subnet of the flight equipment sending the broadcasts. If using UDP multicasting, GSE must subscribe to the multicast group that the gondola network devices are sending multicast traffic to.

If using the CSBF-managed Starlink solution, the gondola network will be connected to the field location mission network via IPSEC IKEv2 VPN. Science devices on either network can communicate via routed IP connectivity as if they were on connected private networks. Note that broadcast and multicast traffic does not traverse this VPN connection.

During integration activities when Starlink or LOS EVTM may be unavailable or turned off, science teams often work with the CSBF Payload Engineer to directly connect the science GSE to the gondola network switch for testing and configuration of the science flight systems. It is recommended for the science GSE to have multiple network interfaces, or to have a science network switch, for making these connections. Work with the CSBF Payload Engineer during mission planning to further discuss the specific details of how interfaces can be used or tested before flight at the field location.

Gondola Network

The CSBF Payload Engineer manages all aspects of the CSBF gondola network.

When using LOS EVTM for data downlink, the gondola network interface will consist of an unmanaged Ethernet switch with RJ45 connectors. As mentioned in the general EVTM section, UDP multicast (preferred) or UDP broadcast are used to traverse the EVTM link from gondola to GSE networks. Flight equipment will send data to either the network subnet broadcast IPv4 IP address or multicast group Ipv4 IP address.

If using the CSBF-managed Starlink solution, the gondola network interface will consist of an unmanaged Ethernet switch with RJ45 connectors, with an upstream industrial router. The CSBF payload engineer will assign an Ipv4 network subnet for science use on the gondola network, including the gateway IP address and subnet mask. Any publicly routable internet destination can be accessed using this network gateway, and the CSBF IPSEC IKEv2 VPN automatically connects the gondola network subnet to the GSE mission network subnet. The Starlink "CSBF-managed" interface section provides additional implementation information.

Example Implementation

For the example, we'll assume a conventional mission in Ft. Sumner, NM (FTS) with both LOS EVTM and a CSBF-managed Starlink interface, with a CSBF CIP controlling flight systems. CIP interfaces are not network-based and thus not discussed in this document. IPv4 addresses and ports given are for demonstration only but represent flight-like configurations.

Telemetry architecture: Science will multicast UDP packets for sending data over LOS EVTM to the science GSE in FTS and unicast UDP packets for sending data over Starlink to the science GSE in FTS.

Gondola Network:
LOS EVTM buffer drain rate: 16Mbps (x 90% = 14.4Mbps data rate available to science)
Network: 10.1.2.0/24
Gateway IP: 10.1.2.1
Subnet mask: 255.255.255.0
Science flight computer IP: 10.1.2.10, has SSH enabled on port 22.
UDP Multicast group IP: 239.255.0.1, science UDP port 6565

The science flight computer is connected to the CSBF ethernet switch on the gondola. The science flight software starts a 14Mbps UDP multicast data stream to multicast group IP 239.255.0.1 port 6565. The science flight computer also starts a 5Mbps UDP unicast data stream to the GSE IP 192.168.90.15, port 6580. The CSBF network equipment connects the LOS EVTM and Starlink data streams to the GSE mission network.

GSE Mission Network:
Network: 192.168.90.0/24
Gateway IP: 192.168.90.1
Subnet mask: 255.255.255.0
Science GSE computer IP: 192.168.90.15
Multicast group IP: 239.255.0.1

The science GSE is connected to the CSBF mission network in FTS. The GSE software has joined multicast group 239.255.0.1 and is listening on port 6565, which receives LOS EVTM UDP data at 14Mbps. The GSE is also listening for UDP data arriving to the GSE IP at port 6580, which receives Starlink UDP data at 5Mbps. A science team member initiates a SSH session to the flight computer IP 10.1.2.10 from the GSE, which the CSBF network equipment routes over the Starlink VPN to the gondola network.

7 LDB Mission Network Configuration

GSE Network

For GSE supporting LDB missions, there is both a field mission network and a Palestine OCC mission network. The mission network located at the field location is used for science GSE supporting launch operations and LOS data collection. The Palestine OCC mission network is used for science GSE supporting flight operations and OTH data collection.

In both locations, critical GSE are typically given static IPv4 IP address reservations based on their hardware MAC addresses. Other devices use DHCP IPv4 IP address assignment. CSBF IT Support manages all aspects of the field and Palestine OCC mission networks, with collaboration from the CSBF Payload Engineer.

Devices on both mission networks will have outbound internet access by default. If remote access to GSE is requested, CSBF IT Support can provide two options: Sonicwall NetExtender VPN (preferred), or NAT translation/port forwarding firewall rules. The Sonicwall NexExtender VPN requires that the remote client can run the NetExtender VPN client. The NAT translation option maps a CSBF public IPv4 IP address and port combination to the GSE's private IPv4 address and port and allows this access to a defined set of remote public IPv4 IP addresses/ranges of addresses only (typically a home institution).

LOS EVTM telemetry will be returned to the field mission network. As mentioned in the general EVTM section, UDP multicast (preferred) or UDP broadcast are used to traverse the EVTM link from gondola to GSE networks. If using UDP broadcasting, the GSE equipment subnet mask must overlap with the IPv4 subnet of the flight equipment sending the broadcasts. If using UDP multicasting, GSE must subscribe to the multicast group that the gondola network devices are sending multicast traffic to.

TDRSS EVTM (if available) telemetry will be returned to the Palestine OCC mission network. The same considerations described for LOS EVTM also apply to TDRSS EVTM otherwise. In cases where LOS EVTM and TDRSS EVTM are both utilized, IPv4 UDP multicast group IPs are used in conjunction with multicast filtering by the CSBF network equipment to distinguish which link is used for data being sent from the gondola. For example, 239.255.0.1 may be used for LOS EVTM while 239.255.0.2 may be used for TDRSS EVTM.

The CSBF Payload Engineer will assign these groups and can work with the science team on any implementation specific details or concerns.

If using the CSBF-managed Starlink solution, the gondola network will be connected to the Palestine OCC mission network via IPSEC IKEv2 VPN. Science devices on either network can communicate via routed IP connectivity as if they were on connected private networks. Note that broadcast and multicast traffic does not traverse this VPN connection.

During integration activities when Starlink or LOS EVTM may be unavailable or turned off, science teams often work with the CSBF Payload Engineer to directly connect the science GSE to the gondola network switch for testing and configuration of the science flight systems. It is recommended for the science GSE located in the field to have multiple network interfaces, or to have a science network switch, for making these connections. Work with the CSBF Payload Engineer during mission planning to further discuss the specific details of how interfaces can be used or tested before flight at the field location.

Gondola Network

The CSBF Payload Engineer manages all aspects of the CSBF gondola network.

When using LOS EVTM for data downlink, the gondola network interface will consist of an unmanaged Ethernet switch with RJ45 connectors. As mentioned in the general EVTM section, UDP multicast (preferred) or UDP broadcast are used to traverse the EVTM link from gondola to GSE networks. Flight equipment will send data to either the network subnet broadcast IPv4 IP address or multicast group IPv4 IP address.

If using TDRSS EVTM with LOS EVTM, the gondola network interface will consist of a managed Ethernet switch with RJ45 connectors.

If using the CSBF-managed Starlink solution, the gondola network interface will consist of an Ethernet switch with RJ45 connectors, with an upstream industrial router. The CSBF payload engineer will assign an IPv4 network subnet for science use on the gondola network, including the gateway IP address and subnet mask. Any publicly routable internet destination can be accessed using this network gateway, and the CSBF IPSEC IKEv2 VPN automatically connects the gondola network subnet to the Palestine OCC mission network subnet. The Starlink "CSBF-managed" interface section provides additional implementation information.

Example Implementation

For the example, we'll assume an LDB mission in Antarctica (ANT) with both LOS EVTM, TDRSS EVTM, and a CSBF-managed Starlink interface, with a CSBF SIP controlling flight systems. SIP interfaces are not network-based and thus not discussed in this document. IPv4 addresses and ports given are for demonstration only but represent flight-like configurations.

Telemetry architecture: Science will multicast UDP packets for sending data over LOS EVTM to the science GSE in ANT, separately multicast UDP packets for sending data over TDRSS EVTM to the science GSE at the Palestine OCC, and unicast UDP packets for sending data over Starlink to the science GSE at the Palestine OCC. In the example, CSBF also uses the TDRSS EVTM channel to send telemetry to the Palestine OCC at 5Kbps. TDRSS EVTM data rates are subject to scheduled availability, satellite, and other factors, but 150Kbps is assumed to be available for the example.

Gondola Network:

LOS EVTM buffer drain rate: 16Mbps (x 90% = 14.4Mbps data rate available to science)
TDRSS EVTM buffer drain rate: 150Kbps (x 90% = 135 Kbps – 5Kbps CSBF TM = 130Kbps data rate available to science).
Network: 10.1.2.0/24
Gateway IP: 10.1.2.1
Subnet mask: 255.255.255.0
Science flight computer IP: 10.1.2.10, has SSH enabled on port 22.
UDP Multicast group IP: 239.255.0.1 for LOS EVTM, 239.255.0.2 for TDRSS EVTM, science UDP port 6565 and 6570 respectively.

The science flight computer is connected to the CSBF Ethernet switch on the gondola. The science flight software starts a 14Mbps UDP multicast data stream to multicast group IP 239.255.0.1 port 6565 and starts a 130Kbps UDP multicast data stream to multicast group IP 239.255.0.2 port 6570. The science flight computer also starts a 2Kbps UDP unicast data stream to the GSE IP 192.168.90.15, port 6580. The CSBF network equipment connects the LOS EVTM data stream to the field mission network, and the TDRSS EVTM and Starlink data streams to the Palestine OCC mission network.

Field GSE Mission Network
Network: 172.20.20.0/24
Gateway IP: 172.20.20.1
Subnet mask: 255.255.255.0
Science GSE computer IP: 172.20.20.20
Multicast group IP: 239.255.0.1
The science GSE is connected to the CSBF mission network in ANT. The GSE software has joined multicast group 239.255.0.1 and is listening on port 6565, which receives LOS EVTM UDP data at 14Mbps.

Palestine OCC Mission Network:
Network: 192.168.90.0/24
Gateway IP: 192.168.90.1
Subnet mask: 255.255.255.0
Science GSE computer IP: 192.168.90.15
Multicast group IP: 239.255.0.2

The science GSE is connected to the CSBF Palestine OCC mission network. The GSE software has joined multicast group 239.255.0.2 and is listening on port 6570, which receives TDRSS EVTM UDP data at 130Kbps. The GSE is also listening for UDP data arriving to the GSE IP at port 6580, which receives Starlink UDP data at 2Kbps. A science team member initiates a SSH session to the flight computer IP 10.1.2.10 from the GSE, which the CSBF network equipment routes over the Starlink VPN to the gondola network.

8 APPENDIX

8.1 NETWORK TOOLS

The following network testing tools have proven to be invaluable in testing various network related configurations or troubleshooting networking issues.

iPerf 2 – Network Performance Measurement

iPerf is open-source software for performing network performance testing. CSBF uses iPerf 2 primarily for sending and receiving UDP multicast frames over EVTM to test flight configurations. Note that iPerf version 2 has better support for multicasting, whereas iPerf 3 is better suited to unicast testing.

Wireshark – Packet Analyzer Software

Wireshark is open-source packet analyzing software. CSBF uses Wireshark when troubleshooting network related issues. By capturing and filtering network packets with Wireshark, underlying network configuration or device issues can be investigated.

midBitTech SharkTapBYP – Ethernet Packet Sniffer Hardware

SharkTapBYP makes capturing Ethernet frames with Wireshark much easier, and without changing the network configuration for your host device. The SharkTapBYP device can be powered and connected via USB3 without drivers required on Windows or most Linux operating systems. It appears as a network interface to Wireshark or other tools.

Graphical Network Simulator 3 (GNS3)

GNS3 is an open-source network software emulator which allows for simulation of complete network implementations. GNS3 can also interface with physical hardware to simulate portions of a network link. The simulator can run various popular hardware firmware, such as Mikrotik Router OS, as well as built-in generic hardware.

Mikrotik Physical Hardware / Router OS

Mikrotik router hardware running Router OS is an inexpensive way to experiment with networking hardware or network configurations. Mikrotik Router OS is a proprietary, closed-source operating system for network equipment. Mikrotik hardware comes with an unlimited Router OS license, or it can be downloaded in CHR or Cloud Hosted Router form and run on virtual machines, or GNS3 with licensed tiers for speed limit (up to 1Mbit free).

8.2 EVTM SIMULATED TESTING

Requirements

1. 2x laptops with ethernet adapters
2. 2x ethernet cables
3. 1x unmanaged network switch supporting multicast frames/groups, with at least 2 ports. If using a managed switch with IGMP snooping enabled, ensure multicast is forwarded appropriately or disable snooping for the test.

4. iPerf version 2 (2.0.8 used in examples) installed on each laptop
5. Wireshark packet analyzer software (4.0.3 used in examples)

Setup

1. One laptop will simulate being a gondola flight computer, while the other will simulate being a GSE computer.
2. Connect each laptop to the ethernet switch using ethernet cables. Turn off Wi-Fi or other network adapter connections which are not involved in the test.
3. Set up a static IP address on each laptop, for example:
    a. Flight computer
        i. IP: 192.168.0.10
        ii. Gateway: 192.168.0.1
        iii. Subnet mask: 255.255.255.0
    b. GSE computer
        i. IP: 192.168.0.20
        ii. Gateway: 192.168.0.1
        iii. Subnet mask: 255.255.255.0
4. On each laptop, open a terminal / command prompt and navigate to the directory where iPerf is installed (if running Windows).

Running an iPerf test

1. On the GSE laptop, type the following command into the command prompt window and hit enter:

    iperf -s -u -B 239.255.0.1 -i 1 -p 6565
    a. The iPerf server will start listening for incoming UDP packets sent to the multicast group 239.255.0.1 at port 6565, and report statistics every 1 second once traffic is sent.
2. On the flight computer laptop, type the following command into the command prompt window and hit enter:
    iperf -c 239.255.0.1 -u -t 15 -i 1 -b 10M -p 6565
    a. The iPerf client will send UDP packets to the multicast group 239.255.0.1 for 15 seconds at a rate of 10Mbps to port 6565, and report statistics every 1 second.
3. If the GSE laptop ("iPerf server") successfully receives the UDP traffic being sent by the flight computer laptop ("iPerf client"), the laptops are successfully configured for continuing to test.
4. If you don't see traffic, temporarily disable Windows Firewall / Linux firewall on the test interface or allow iPerf/UDP on the chosen port.

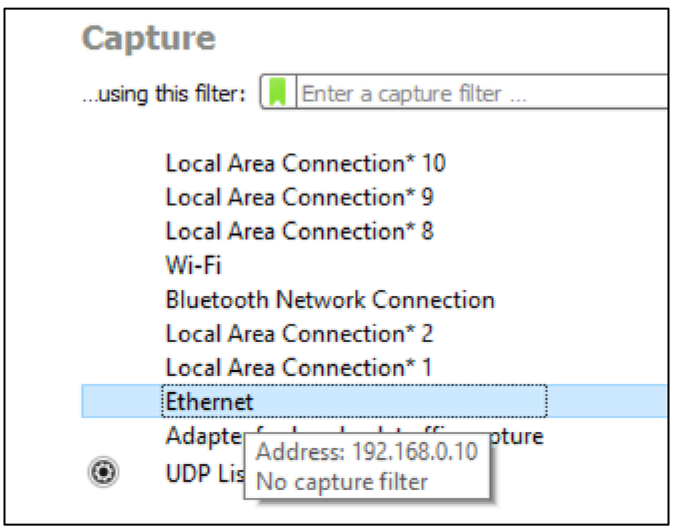
Simulating science data transmission over EVTM link

1. Simulating science data transmission follows a similar path as the iperf section above.
2. Set up the GSE and flight computer with static IP addresses and network configuration as in the iPerf testing section.
3. On the GSE system, have your ground software bind the ethernet adapter to the multicast group **239.255.0.1**, and have your software listen for UDP traffic on a port of your choosing (64646 was used in the iPerf example).
4. On the flight computer, configure your flight software to send telemetry/data via UDP to the multicast group **239.255.0.1**, on the port from step 3 above.
5. Confirm UDP telemetry/data packets are received on your GSE system.

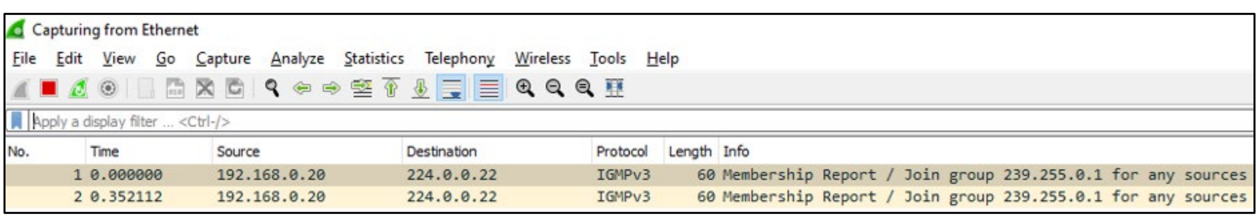
6. If successful, your flight computer and GSE are properly configured for interfacing with the CSBF EVTM system. During planning for integration and flight, we will work with you to agree on the actual IP address and ports to be used in flight.
7. Note, if TDRSS **and** line of sight (LOS) transmitters will be used (such as on an LDB flight), your flight software ***must*** be able to:
   a. Switch telemetry between one of two multicast IPs upon request (when switching from one link path to the other)
   b. Adjust telemetry/ data rate to match the previously agreed upon bandwidth budgets for the link (TDRSS has less bandwidth than LOS)
   c. Alternatively, two data streams can be sent, one to each multicast group (one for TDRSS, one for LOS), with the data rate of each set to the previously agreed upon bandwidth limits.

Capturing multicast traffic using Wireshark

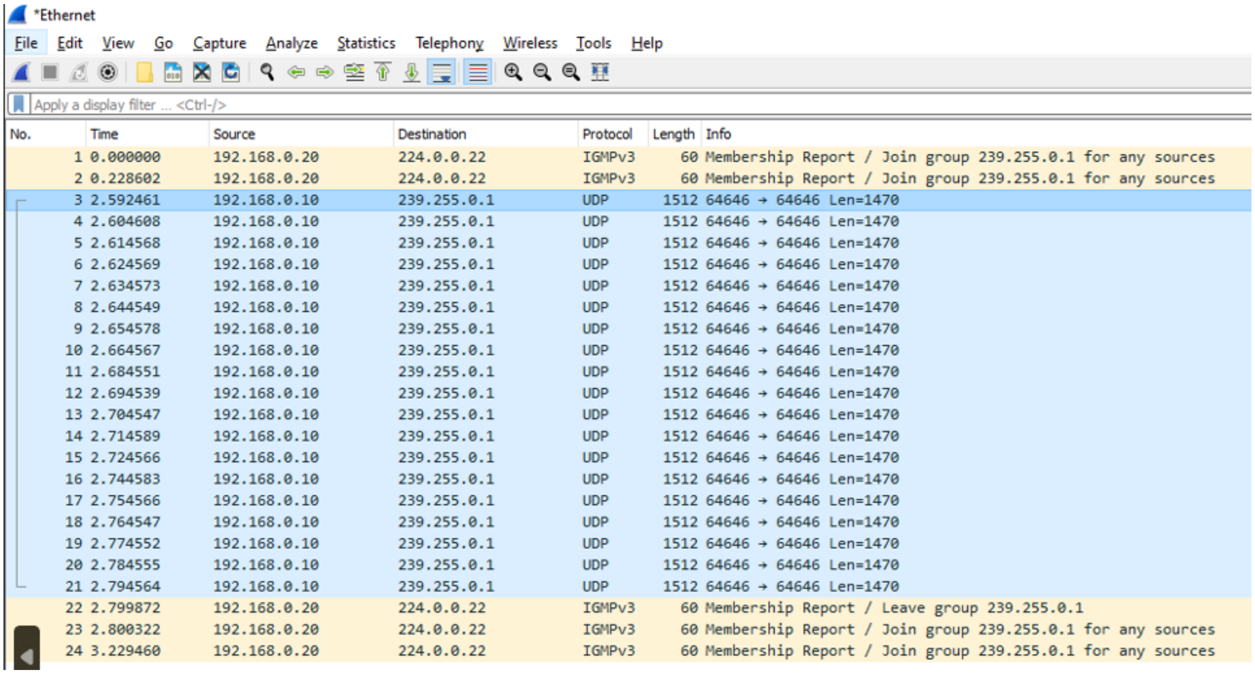
1. Setup is the same as shown in the "Setup" section. The example will capture iPerf UDP traffic.
2. On one of the two computers, or another computer connected to the same ethernet switch, install Wireshark packet analyzer software.
3. Launch Wireshark and double click on the interface connected to the ethernet switch to begin recording network traffic. In the following screenshot the "Ethernet" interface will be utilized:



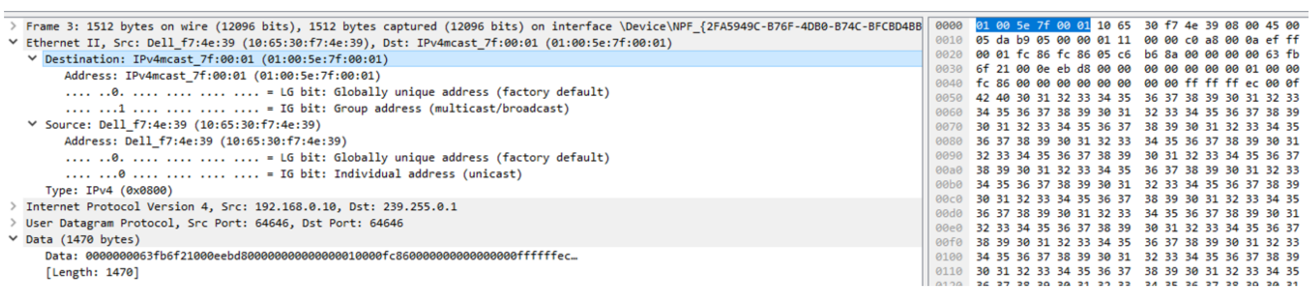
4. Start the iperf server as shown in the "Running an iPerf test" section. Note Wireshark will show the server/GSE laptop attaching to the multicast group:



5. Send UDP traffic from the client/Flight Computer laptop as shown in the "Running an iPerf test" section. Note, Wireshark will show the UDP packets being sent across the network, as well as the devices joining/leaving the multicast group. You may need to further filter the captured traffic if other devices are actively using this network.



6. At this point, the Wireshark capture can be stopped by clicking the red square at the left of the toolbar. By clicking on each UDP packet (shown in the blue section above), the data payload, UDP/Ethernet headers, checksum values, and length can be investigated using the interface in the lower half of the Wireshark capture window.
7. As an example, after clicking on a UDP packet, then selecting Ethernet II>Destination, the correct multicast destination address is shown (multicast MAC 01:00:5E:7F:00:01 is derived from the multicast IP address 239.255.0.1, see http://www.dqnetworks.ie/toolsinfo.d/multicastaddressing.html)



8. Wireshark can also be used to confirm science UDP data is being sent to the correct multicast address, to see ethernet and UDP header information, or to capture the raw science data payload.
9. The Wireshark menu item Statistics -> Conversations can be used to identify Ethernet, TCP/IP, or UDP frame throughput by device during network utilization. This is a great way to understand how much network overhead is being added to your data for Ethernet framing. This is helpful for determining maximum data rate that can be sent through an EVTM (or other) channel, which is given in absolute terms (i.e. EVTM maximum rate = data rate + framing overhead).