

EVTM Simulated Testing

Requirements

- 1. 2x Windows laptops with ethernet adapters
- 2. 2x ethernet cables
- 3. 1x unmanaged network switch supporting multicast frames/groups, with at least 2 ports
- 4. iperf version 2.0.8 installed on each laptop
 - a. Software: <u>https://sourceforge.net/projects/iperf2/</u>
 - b. Manual: <u>https://iperf2.sourceforge.io/iperf-manpage.html</u>
- 5. Wireshark packet analyzer software (4.0.3 used in examples)
 - a. Software: <u>https://www.wireshark.org/</u>

Setup

- 1. One laptop will simulate being a flight computer, while the other will simulate being a ground support equipment (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 command prompt and navigate to the directory where iperf is installed.

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 64646**
 - The iperf server will start listening for incoming UDP packets sent to the multicast group
 239.255.0.1 at port 64646, 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 3 -t 15 -i 1 -b 10M -p 64646 -B 192.168.0.10:64646**
 - 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 64646, 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. If iperf data is not being transferred successfully, confirm network settings, cables, and switch power and try again.

Simulating science data transmission over EVTM link

1. Simulating science data transmission follows a similar path as the iperf section above.

Title:	EVTM Simula	ted Testing		Page: 2 of 3	* + K
Revision:	А		Document Date:	02/26/2023	PRINE THE

- 2. Setup the GSE and flight computer with static IP addresses and network configuration as in the iperf testing section.
- 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. The typical IP range given to science is 192.168.1.X, with gateway 192.168.0.1, and subnet mask 255.255.0.0.
- 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 particular 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. Set up 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.
- 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:

Cap	ture
using	g this filter: 📔 Enter a capture filter
	Local Area Connection* 10
	Local Area Connection* 9
	Local Area Connection* 8
	Wi-Fi
	Bluetooth Network Connection
	Local Area Connection* 2
	Local Area Connection* 1
	Ethernet
۲	Adapte Address: 192.168.0.10 UDP Lis No capture filter

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:

Title:	EVTM Simula	ted Testing		Page: 3 of 3	
Revision:	А		Document Date:	02/26/2023	THE TOP

+

🙍 Capti	Capturing from Ethernet						
<u>F</u> ile <u>E</u>	dit <u>V</u> iew <u>G</u> o	<u>Capture Analyze Stat</u>	istics Telephon <u>y W</u> ireless	s <u>T</u> ools <u>H</u>	elp		
	■ ③ □ □ □ 🗠 🖄 🖾 । ९. ⇔ 🕾 🗿 👲 🚍 🔍 ९. ९. ९. ୩						
Apply a display filter <ctrl-></ctrl->							
No.	Time	Source	Destination	Protocol	Length	Info	
	1 0.000000	192.168.0.20	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.0.1 for any sources	
	2 0.352112	192.168.0.20	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.0.1 for any sources	

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:

	🚄 *Ethernet						
Ei	e <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u>	atatistics Telephony <u>W</u> ireles	s <u>T</u> ools <u>H</u>	elp		
	🔳 🔬 💿 📙 📑	🔀 🖾 ९ 👄 🔿	🕾 T 🕹 📑 🔳 Q Q	Q. 🎹			
	Apply a display filter <0	Ctrl-/>					
No	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	192.168.0.20	224.0.0.22	IGMPv3	60 Membership Report / Join group 239.255.0.1 for any sources		
	2 0.228602	192.168.0.20	224.0.0.22	IGMPv3	60 Membership Report / Join group 239.255.0.1 for any sources		
	3 2.592461	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	4 2.604608	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	5 2.614568	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	6 2.624569	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	7 2.634573	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	8 2.644549	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	9 2.654578	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	10 2.664567	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	11 2.684551	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	12 2.694539	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	13 2.704547	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	14 2.714589	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	15 2.724566	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	16 2.744583	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	17 2.754566	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	18 2.764547	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	19 2.774552	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	20 2.784555	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
L	21 2.794564	192.168.0.10	239.255.0.1	UDP	1512 64646 → 64646 Len=1470		
	22 2.799872	192.168.0.20	224.0.0.22	IGMPv3	60 Membership Report / Leave group 239.255.0.1		
	23 2.800322	192.168.0.20	224.0.0.22	IGMPv3	60 Membership Report / Join group 239.255.0.1 for any sources		
	24 3.229460	192.168.0.20	224.0.0.22	IGMPv3	60 Membership Report / Join group 239.255.0.1 for any sources		

- 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.
- 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 heater information, or to capture the raw science data payload.