Aerospace Village – Deep Space Networking Workshop #2

Recommended Steps and Hints

To help you work your way through the *tcpcl_we2ereceipt.pcap* trace file, I've jotted down some steps you may want to take to identify the bundle that is being relayed using the Bundle protocol and TCP Convergence Layer.

1. Look through the trace file to get a feel for the traffic. It's only 122 packets, so that shouldn't take long.
2. The OSPF traffic is not part of the DTN (Delay and Disruption Tolerant Networking) traffic. Filter it from view using `!ospf`.
3. Check out the UDP traffic to/from port 5656. Note the sending IP address and the payload in the Packet Bytes window. There are several Endpoint IDs visible in the payload (n1, n2…).
4. This trace file contains a bundle that is being sent from one host through a relay to another host. We want to focus on the two most active TCP connections. Check out the **Statistics | Conversations** window for this information and build a filter to show these two conversations.
5. Once you have the two most active conversations in view, save a new trace file containing only this traffic (**File | Export Specified Packets**). Call your new file *DTN-example.pcapng*.
6. Open your *DTN-example.pcapng*.
7. Look at the TCPCL Keepalive packets. You can build your interplanetary network diagram from this information. You will be able to determine which hosts can communicate with each other.
8. Note the bundle segments identified in the Info column. Click on these packets and examine their contents. Within the TCPCL header, you will find the Packet Type, Start of Bundle bit, and the End of Bundle bit. Right click on each of these fields and add them as columns.
9. Consider creating coloring rules on these fields (right click on the field and select **Colorize | New Coloring Rule**). Remember that packets are processed in order through the Coloring Rules list. In the video, I set the Start of Bundle packets to a green background, the End of Bundle packets to a red background, and the Bundle Status Report to a yellow background.
10. You may also want to create display filter buttons based on the Start of Bundle and End of Bundle fields. Right click on the field and select **Prepare as Filter | Selected** and name your button.
11. Consider jotting down notes on the source and destination IP addresses in the bundle segment packets and you'll find the first bundle, second bundle, and then an administration report packet.

Enjoy!

Laura Chappell
Founder, Chappell University
laura@chappellU.com