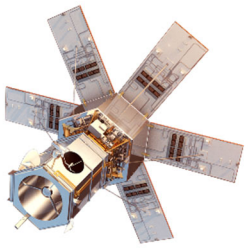
Aerospace Village

Deep Space Networking Challenge #3



Authors: Laura Chappell, Chappell University
Ginny Spicer, Chappell University

Trace File: *dtn-contact2conv.pcapng*

The trace file referenced in Deep Space Networking Challenges #1 and #2 did not depict the connection establishment process. Let's look at that.

Using *dtn-contact2conv.pcapng*, answer the following questions.

1. What must occur before hosts can send Contact Headers to each other?

2. What Wireshark display filter can be used to detect Contact Header packets?

3. Are Contact Headers part of the TCP-CL protocol or Bundle Protocol?

4. Only one connection is used for data transfer. How can you identify the connection used for data transfer vs. the connection **not** used for data transfer?

5. What is the Keep Alive value advertised by each host seen in the trace file? At what point will the connections be terminated due to Keep Alive timeout? (Consider check the RFC 7242 on this one.)

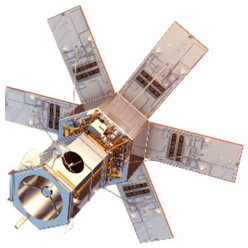
6. If you created the coloring rules depicted in the video (*Analysis of tcpcl_we2ereceipt.pcap*), why don't you see a green Start-of-Bundle packet at the beginning of the conversation containing data?

7. What does the high-order bit of the Bundle Protocol Block Processing Control Flags indicate? (Ouch… this could be a tough one… he he he.)

Answers are located on the next pages.

Aerospace Village

Deep Space Networking Challenge #3



Authors: Laura Chappell, Chappell University
Ginny Spicer, Chappell University

Trace File: *dtn-contact2conv.pcapng*

Answers

1. **What must occur before hosts can send Contact Headers to each other?**
   Hosts must successfully complete the TCP handshake process before sending Contact Headers to each other.

2. **What Wireshark display filter can be used to detect Contact Header packets?**
   There are various display filters that can be used to detect Contact Header packets. The simplest one is likely just `tcpcl.contact_hdr.magic`.

3. **Are Contact Headers part of the TCP-CL protocol or Bundle Protocol?**

   Contact Headers are part of the TCP-CL protocol (defined in RFC 7242, "DTN TCP Convergence Layer).

4. **Only one connection is used for data transfer. How can you identify the connection used for data transfer vs. the connection *not* used for data transfer?**
   You can apply a display filter for `bundle`. The Bundle Protocol header will only appear at the start of data transferred using the Bundle Protocol.

5. **What is the Keep Alive value advertised by each host seen in the trace file? At what point will the connections be terminated due to Keep Alive timeout? (Consider check the RFC 7242 on this one.)**
   The Keep Alive value advertised in all the Contact Headers in the trace file is 15 seconds. Section 5.6 of RFC 7242 indicates that a timeout will occur after "*no message (KEEPALIVE or other) has been received for at least twice the keepalive_interval, then either party MAY terminate the session by transmitting a one-byte SHUTDOWN message (as described in Table 2) and by closing the TCP connection.*"

6. **If you created the coloring rules depicted in the video (*Analysis of tcpcl_we2ereceipt.pcap*), why don't you see a green Start-of-Bundle packet at the beginning of the conversation containing data?**

   We do not see a green Start of Bundle packet because we created an End of Bundle coloring rule and placed it above the Start of Bundle coloring rule. Frames 17 and 23 (or 15 and 21 with TCP reassembly disabled) have both the Start of Bundle and End of Bundle bits set – this is a one-packet bundle.

7. **What does the high-order bit of the Bundle Protocol Block Processing Control Flags indicate? (Ouch… this could be a tough one… he he he.)**

   According to RFC 5050, the Bundle Protocol uses Self-Delimiting Numeric Values (SDNVs). The Block Processing Control Flags field is an SDNV field. SDNV enables field length to be dynamically defined using the high-order bit of each byte of the field. When the high-order bit of the Block Processing Control Flags field is set to 0, this is the final byte of the field. When the high-order bit of the Block Processing Control Flags field is set to 1, the field continues for at least one more byte.

   SDNVs enables future expansion of the Bundle protocol by allowing fields to grow in size.