# TCP Retransmissions

## How Many Is Too Many?

www.BettyDuBois.com/sf24us

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

**Betty DuBois**

**Packet Detectives**

# Whoami?

Betty DuBois

Capturing, analyzing & teaching packets since **1997**

- I am **still** learning stuff about packets

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

# TCP Packet Loss Recovery Primer

# What Can Cause Packet Loss?

Most common culprits

- Physical issues
  - Bad cable, faulty interface, etc
- Network congestion
  - Queues get full on middleware, packet(s) get dropped

# Clues for Physical Issues

Localized

- Only affecting one host, or connection
- Can be found by looking at bad CRC/FCS statistics

# Clues for Network Congestion

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

## Random

- 1-3 packets lost here or there
- Sprinkled over time like glitter

# Scenario 1
# Timeout Retransmission

# What SEQ # Are You Starting With?

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Each side starts with a **random** 4 byte sequence number

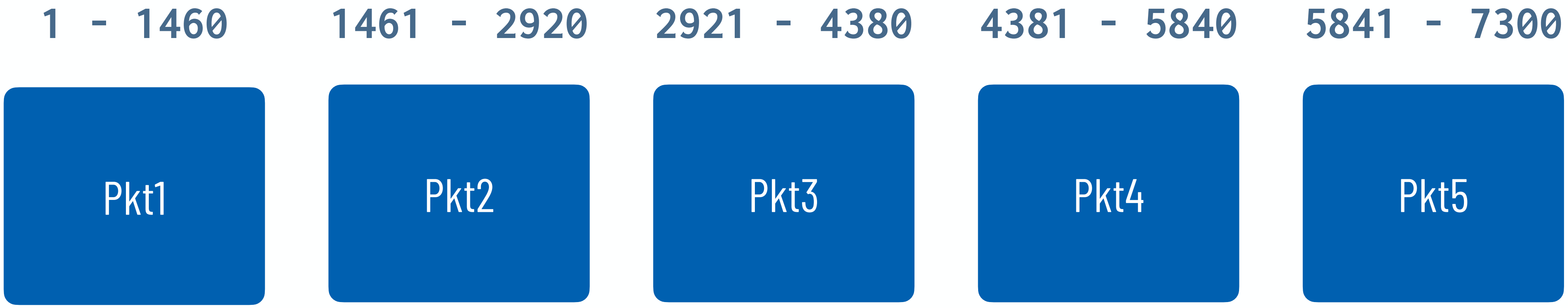
I'm going to start counting at b7 6d d3 b4

Sounds good, I'm going to
start counting at 6e 5c 35 86

# What ACK # to Send?

An ACK is the next expected SEQ #

Seq + TCP Length = Ack Coming Back



| 1 - 1460 | 1461 - 2920 | 2921 - 4380 | 4381 - 5840 | 5841 - 7300 |
|---|---|---|---|---|
| Pkt1 | Pkt2 | Pkt3 | Pkt4 | Pkt5 |

# No ACK?

Time to retransmit

From RFC 6298:

To compute the current RTO, a TCP sender maintains two state variables, SRTT (smoothed round-trip time) and RTTVAR (round-trip time variation)

# Follow Along With Me

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

If you don't have the files - www.bettydubois.com/sf24us

1-starting-example-pcapng

# Verdict?

Expected network loss

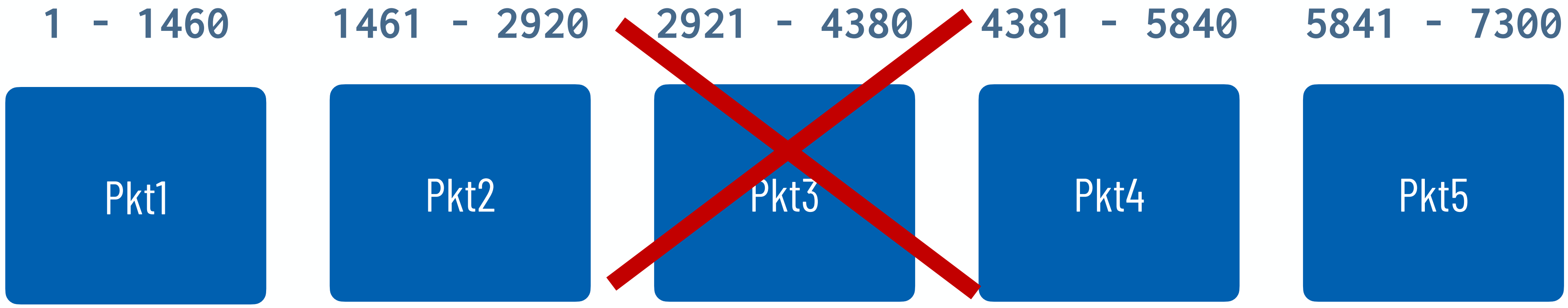
- Did not see the same pattern throughout the entire file
- Recovery happened in a reasonable time

# Scenario 2
# Fast Retransmission

# Receiver Detects Packet Loss

Previous Segment not captured

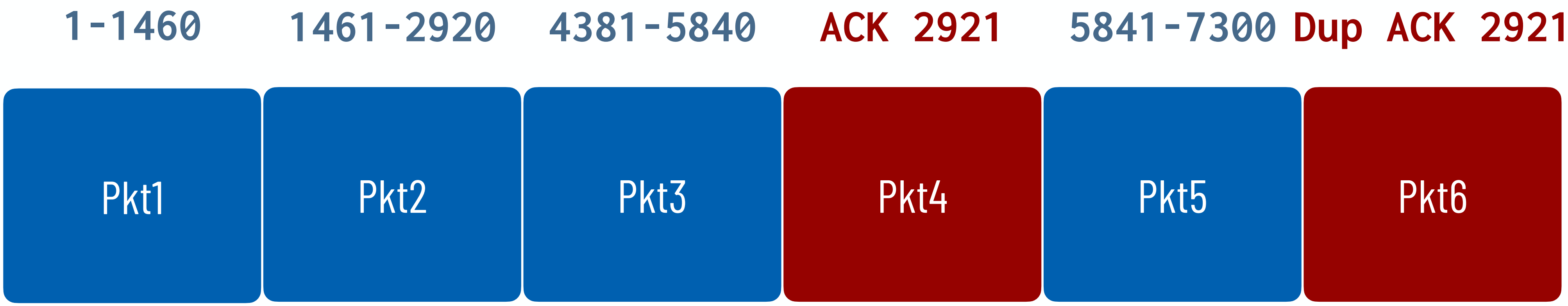
Packet 3 is eaten by the network



# Why Wait? Dup ACKs

Receiver sees the skip in SEQ

Requests the retransmission by ACKing the SEQ it next expects to receive



1-1460
Pkt1

1461-2920
Pkt2

4381-5840
Pkt3

ACK 2921
Pkt4

5841-7300
Pkt5

Dup ACK 2921
Pkt6

# Follow Along With Me

2-packetloss-client.pcapng

3-packetloss-server.pcapng

# Verdict?

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

Expected network loss

- Did not see the same pattern throughout the entire file
- Recovery happened in an expected time
  - Client side - Time between 3rd Dup ACK and Fast Retransmission is less than iRTT
  - Server side - Fast Retransmission after 2nd or 3rd Dup ACK

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

# Scenario 3
# Patterns in Retransmissions

# Patterns

If you see a pattern in the retransmitted packets....

- It is usually something besides expected loss
- See the pattern - See the problem

# Follow Along With Me

3-financial-services-slow-internet.pcapng

Only certain packets are being retransmitted. Which ones?

# Verdict?

## Firewall

Customer later told me that they had started to make use of new threat feeds and it had overwhelmed the firewall

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

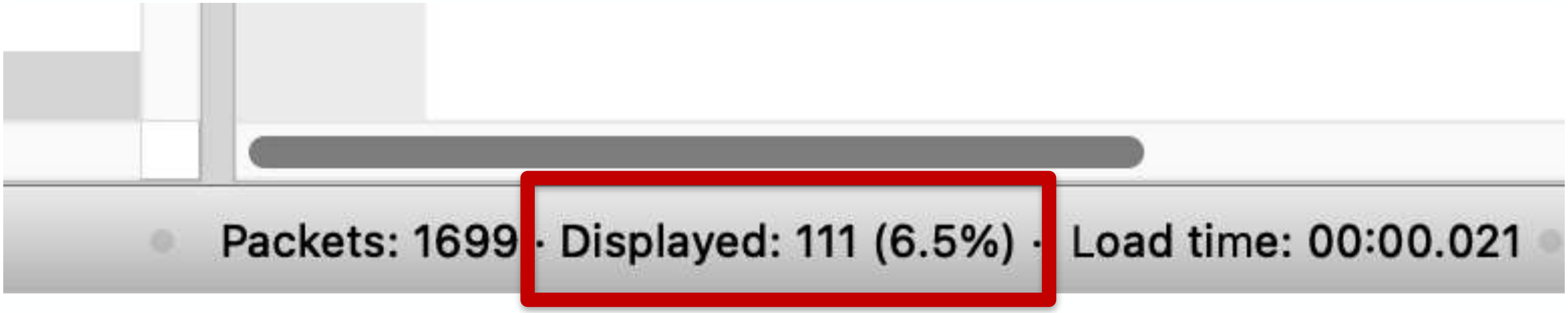
# Scenario 4
# Too Many Retransmissions

# Follow Along With Me

SharkFest'24 US June 15-20 · Fairfax, VA

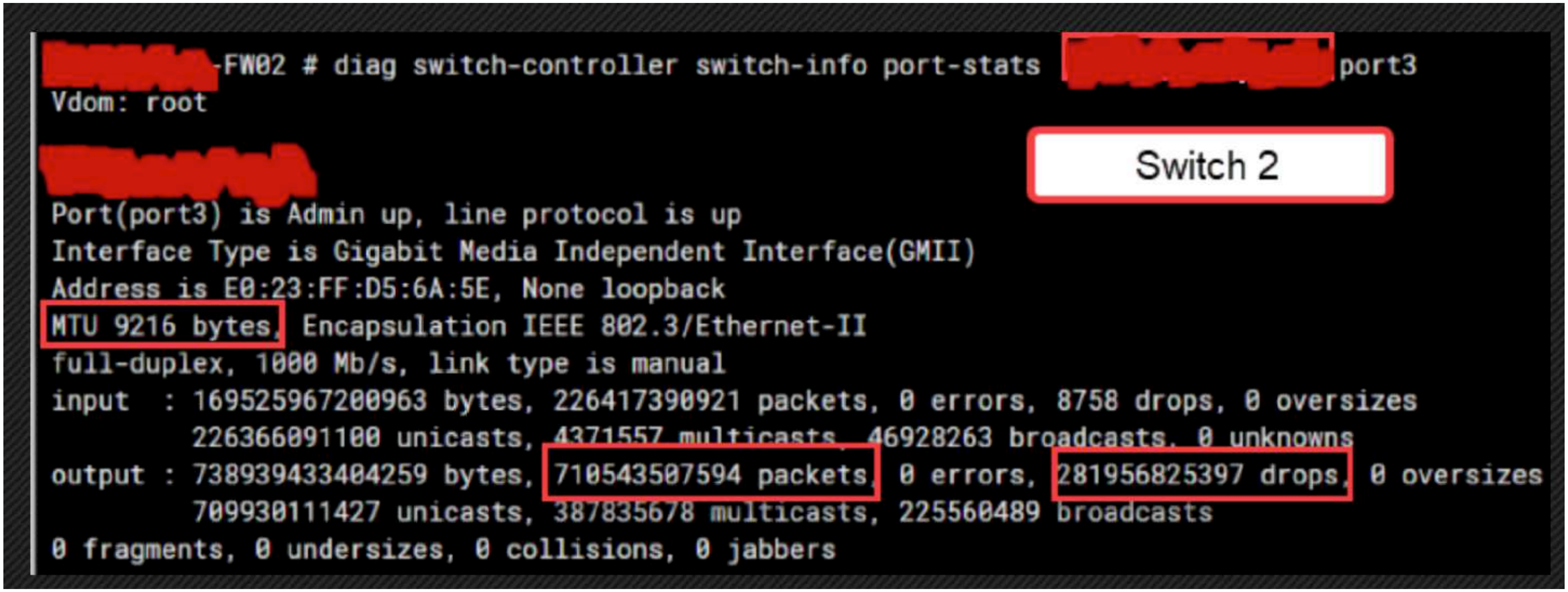
#sf24us

4-slow-logon-DC-side_anon.pcapng



Packets: 1699 · Displayed: 111 (6.5%) · Load time: 00:00.021

# Verdict?



```
[redacted]-FW02 # diag switch-controller switch-info port-stats [redacted] port3
Vdom: root

[redacted]
Port(port3) is Admin up, line protocol is up
Interface Type is Gigabit Media Independent Interface(GMII)
Address is E0:23:FF:D5:6A:5E, None loopback
MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
full-duplex, 1000 Mb/s, link type is manual
input  : 169525967200963 bytes, 226417390921 packets, 0 errors, 8758 drops, 0 oversizes
         226366091100 unicasts, 4371557 multicasts, 46928263 broadcasts, 0 unknowns
output : 738939433404259 bytes, 710543507594 packets, 0 errors, 281956825397 drops, 0 oversizes
         709930111427 unicasts, 387835678 multicasts, 225560489 broadcasts
0 fragments, 0 undersizes, 0 collisions, 0 jabbers
```

Switch 2

# Scenario 5
# Too Many Retransmissions

## Crime

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

Customer is rolling out a new vendor for their warehouse robots

- Developers are complaining about the network because they are seeing "connection lost" messages in their logs

# Follow Along With Me

5-warehouse-st21_anon.pcapng

Is it packet loss?

# Verdict?

Network exonerated!!

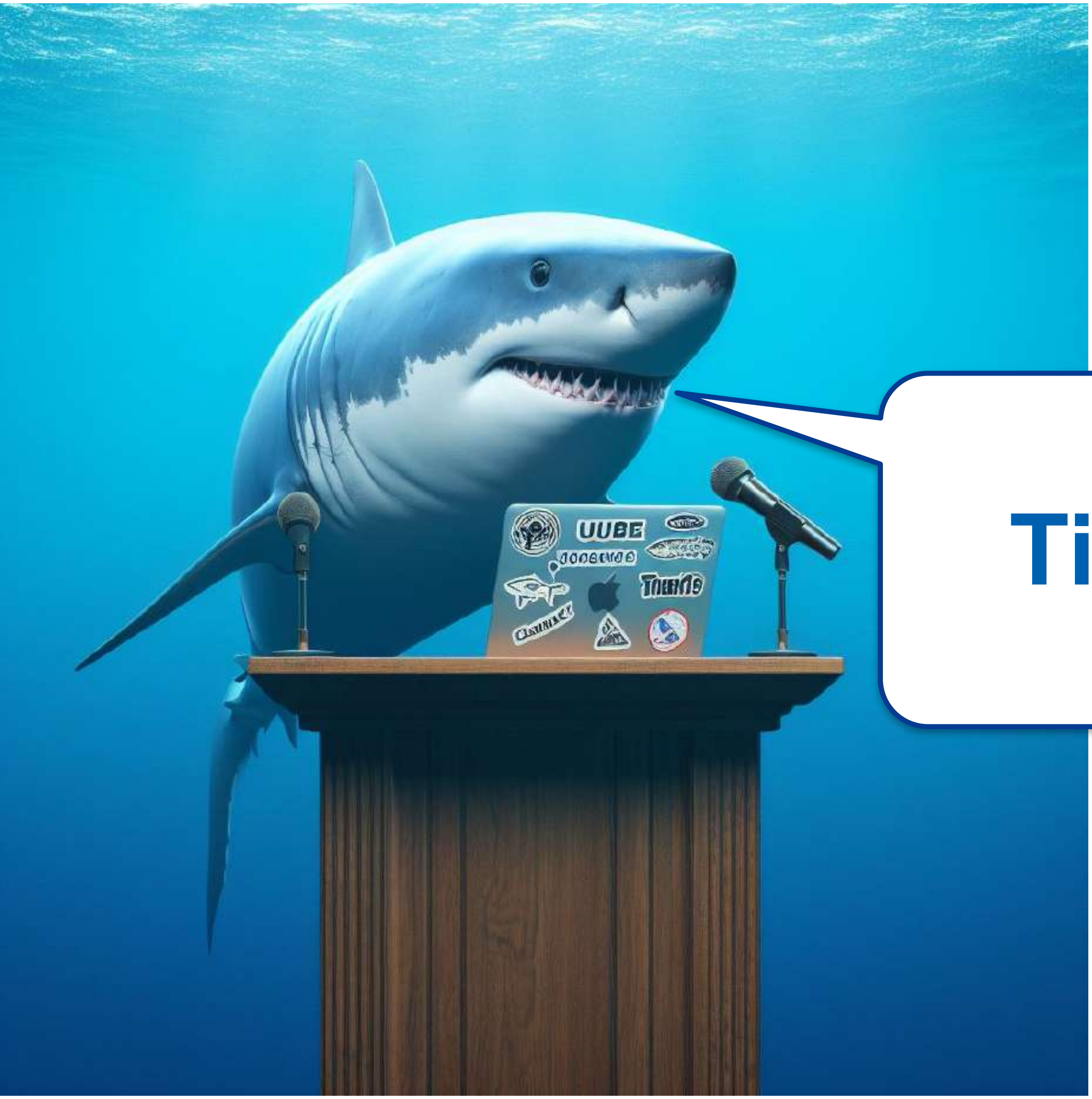
Application layer data is received by PLC, but it's TCP stack does not ACK

PLC is not able to process all of the test traffic

- Modifications were made before the rollout

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



# Time for Q & A

**Generated with Microsoft Designer AI**

**Prompt:** Great white shark, standing at a podium with a laptop. The laptop has stickers on it. Darker blue ocean background.