CHAPPELLUNIVERSITY

Sample Network Analysis Report

Report Information

Report created on 1/9/2014 9:35:19 PM.

Analyst Information

Name	Sample Analysis Report
E-mail Address	info@chappellu.com
Phone Number	408-378-7841

Client Information

Client Name	Chappell University
Case Number	03A543

Table of Contents

IP Conversations

Conversations among IP hosts

Applied on 1/9/2014 9:27:10 PM.

Total capture window: 11/15/2013 18:03:00.533697 - 18:04:30.533697.
Current selection: 11/15/2013 18:03:00.533697 - 18:04:30.533697 (90 s at 1 sec).

Source File: C:\Users\Laura\Documents\Customer Projects\Case 03A543\tr-twohosts.pcapng
File Time: 12/31/2013 4:03:25 PM
File Size: 54525KB
Checksum ():

IP Conversations

VIEW NOTES:
IP host conversations. The size of the host is relative to the amount of data it has transmitted. The size of each connection is relative to how much traffic it has transported between the two endpoints (hosts).

OTHER NOTES:
This trace file contains two conversations. We have two internal hosts that are downloading a file from a remote host. In this report we will refer to the local hosts by the last two bytes of their IP addresses - 1.72 and 1.119. We will refer to the remote server as simply "the remote server."

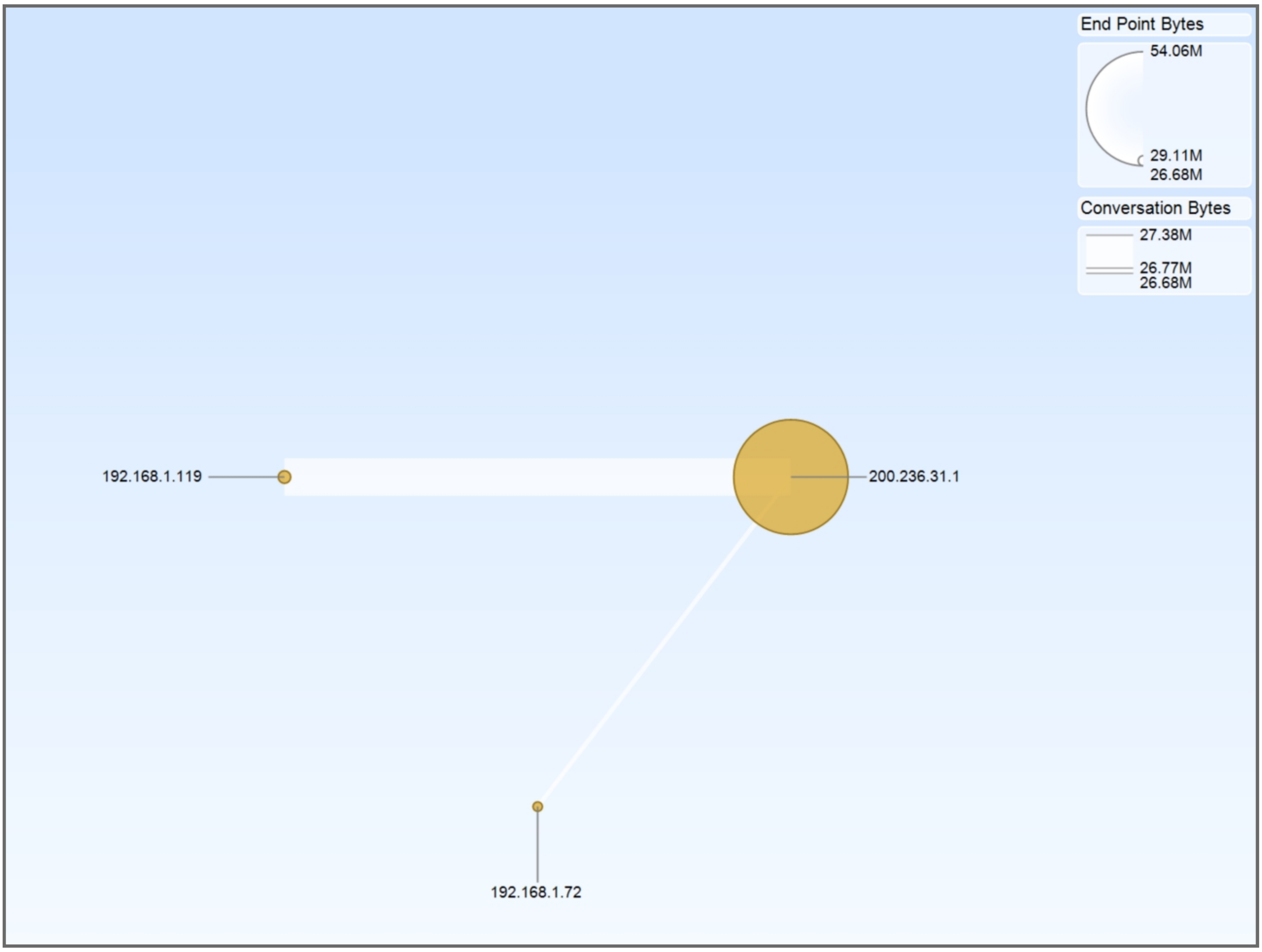

Figure 1 - IP Conversations

Bandwidth Over Time

Total bandwidth over time

Applied on 1/9/2014 9:29:24 PM.

Total capture window: 11/15/2013 18:03:43.415340 - 18:04:30.415340.
Current selection: 11/15/2013 18:03:43.415340 - 18:04:30.415340 (47 s at 1 sec).

Source File: C:\Users\Laura\Documents\Customer Projects\Case 03A543\tr-twohosts.pcapng
File Time: 12/31/2013 4:03:25 PM
File Size: 54525KB
Checksum ():

Drilldown Sequence:

1. Applied the view "IP Conversations"
2. Performed a Conversation selection on the "IP Conversations" Conversation Ring. Details:
   Selected: 200.236.31.1 - 192.168.1.119
3. Applied the view "Bandwidth Over Time"

Bytes per Second

The number of bytes per second.

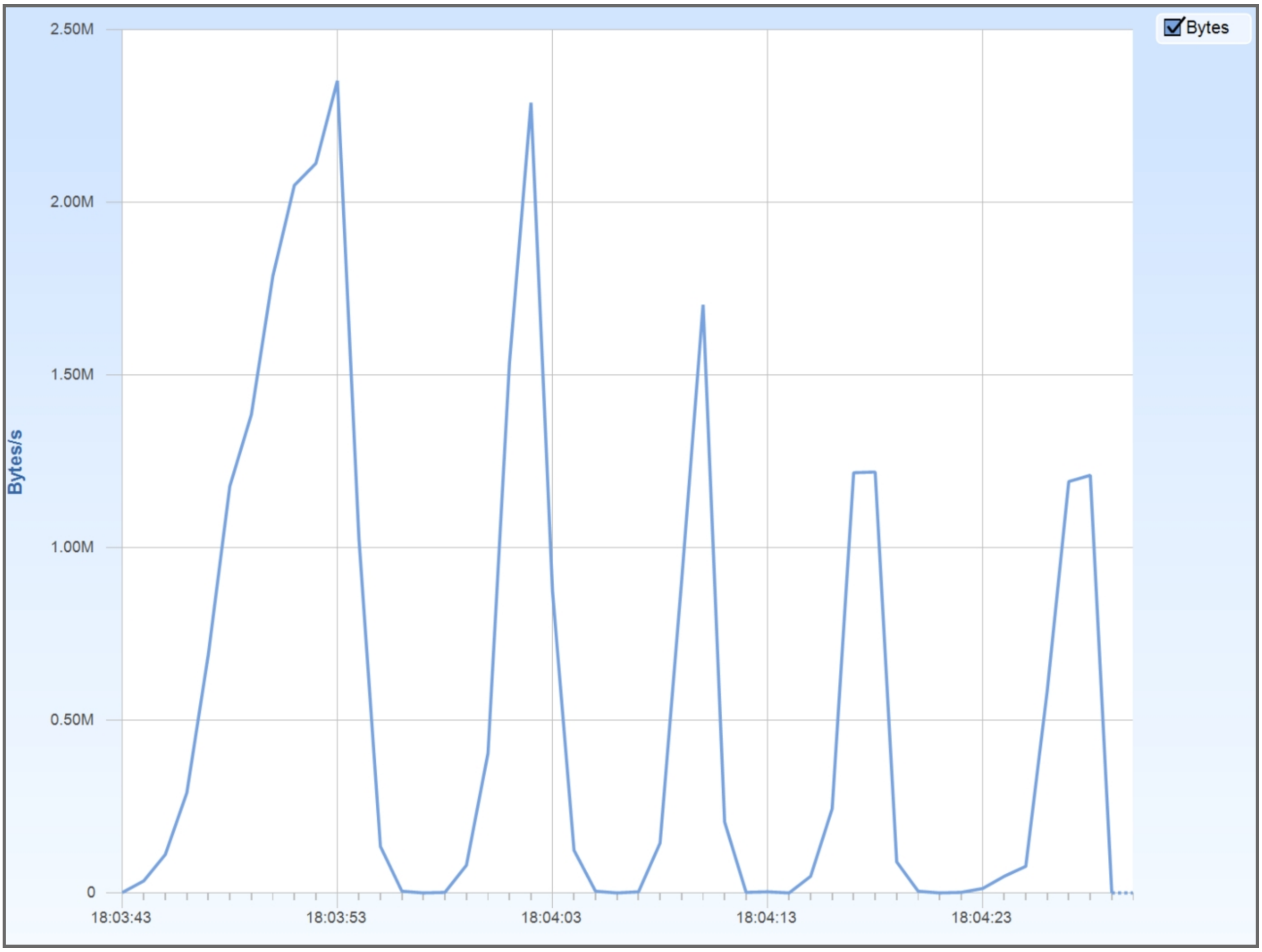

Figure 2 - Bytes per Second

Bits per Second

VIEW NOTES:
The number of bits per second. This enables an at-a-glance view of the total bandwidth used as well as a detailed look in single second precision.

OTHER NOTES:
We applied this "Bandwidth Over Time" view to the traffic to/from 1.119. We can see the throughput reaches 18 Mbps. There are numerous significant drops, however. We will compare this to the throughput graph for traffic to and from 1.72 next. [We used the right-click | drilldown method to create this new view.]

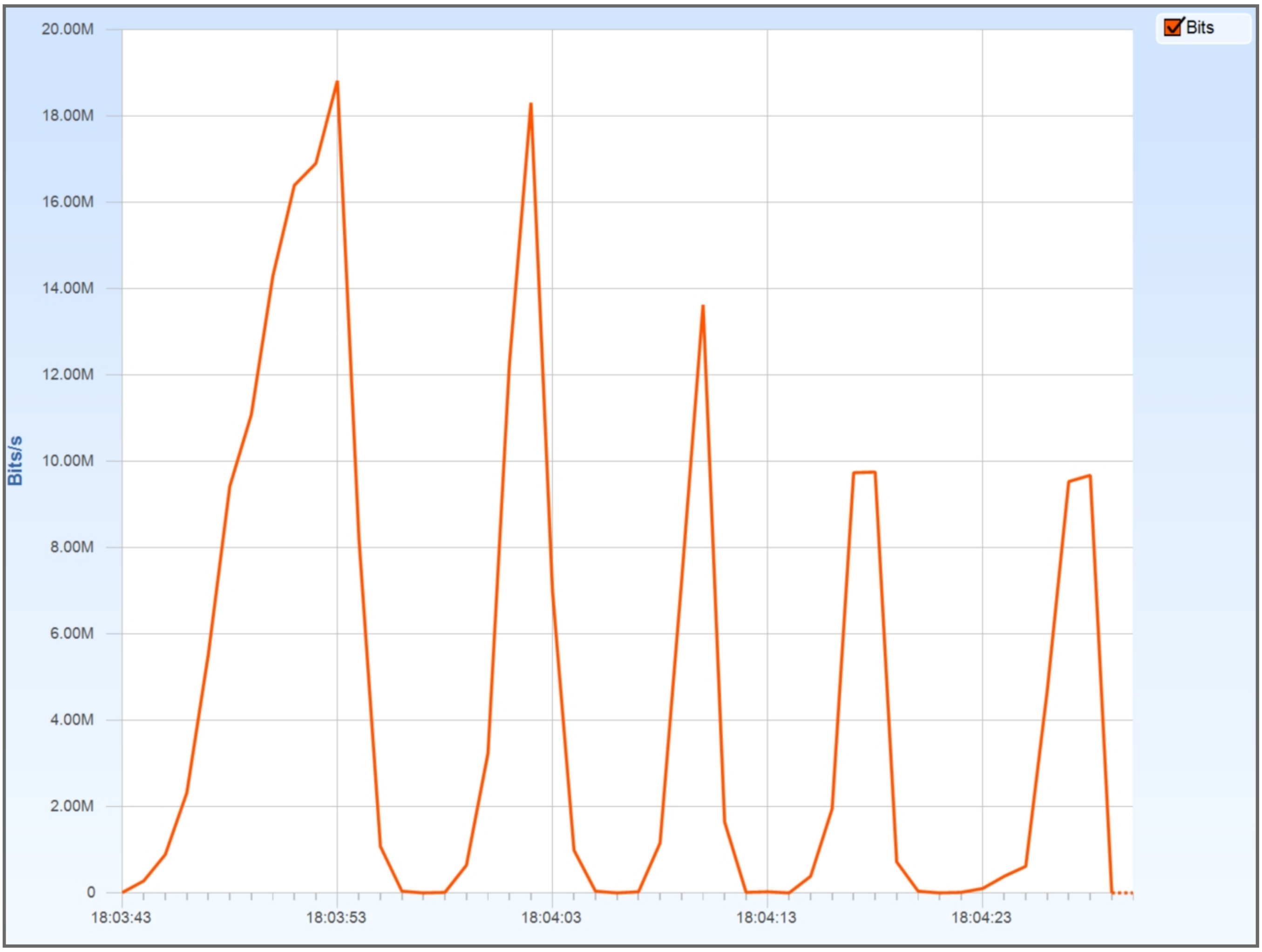

Figure 3 - Bits per Second

Packets per Second

The number of packets per second. This view when compared to the bits/bytes view above allows the user to visually identify when many small packets are generating the traffic or if it is a few larger packets.

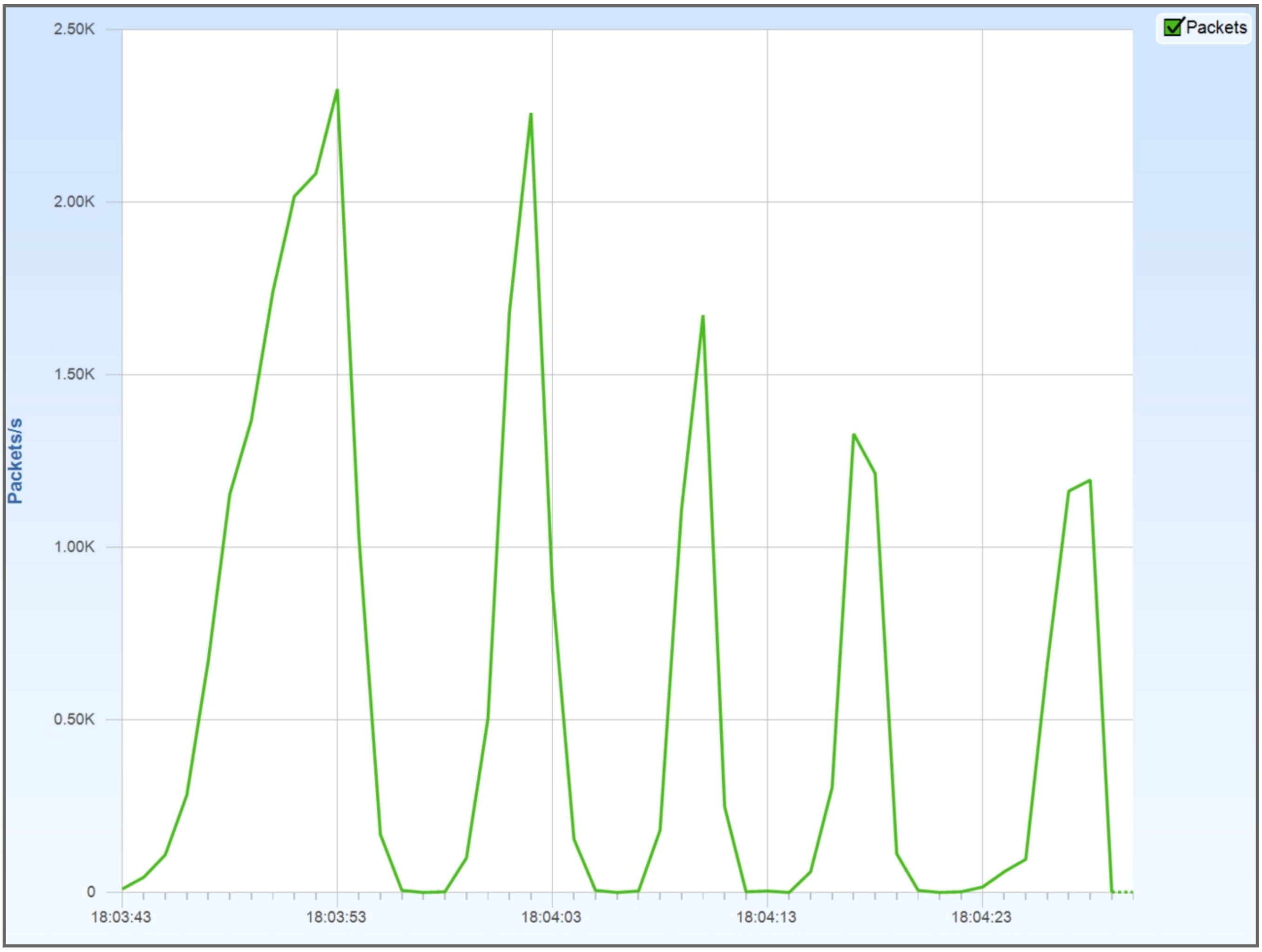

Figure 4 - Packets per Second

Bandwidth Over Time (2)

Total bandwidth over time

Applied on 1/9/2014 9:30:43 PM.

Total capture window: 11/15/2013 18:03:00.533697 - 18:04:02.533697.
Current selection: 11/15/2013 18:03:00.533697 - 18:04:02.533697 (62 s at 1 sec).

Source File: C:\Users\Laura\Documents\Customer Projects\Case 03A543\tr-twohosts.pcapng
File Time: 12/31/2013 4:03:25 PM
File Size: 54525KB
Checksum ():

Drilldown Sequence:

1. Applied the view "IP Conversations"
2. Performed a Conversation selection on the "IP Conversations" Conversation Ring. Details:
   Selected: 200.236.31.1 - 192.168.1.72
3. Applied the view "Bandwidth Over Time (2)"

Bytes per Second

The number of bytes per second.

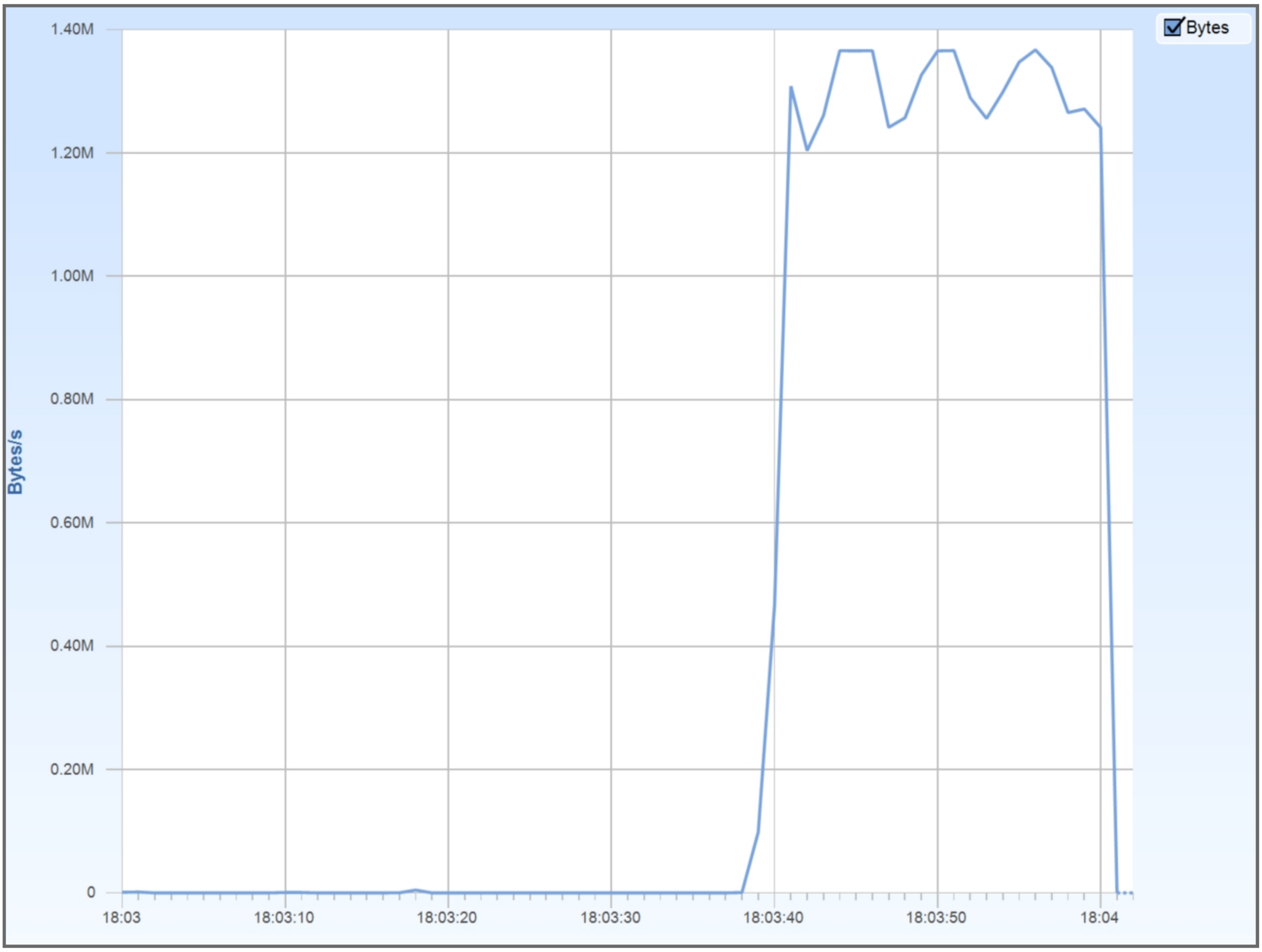

Figure 5 - Bytes per Second

Bits per Second

VIEW NOTES:
The number of bits per second. This enables an at-a-glance view of the total bandwidth used as well as a detailed look in single second precision.

OTHER NOTES:
Interestingly the maximum throughput rate is lower in this IP conversation than the IP conversation to/from 1.119. We can see the consistency of this throughput during the file download to 1.72. Next we want to look further into the 1.119 views to determine if we are dealing with a network issue. [We used the right-click | drilldown method to create this new view.]

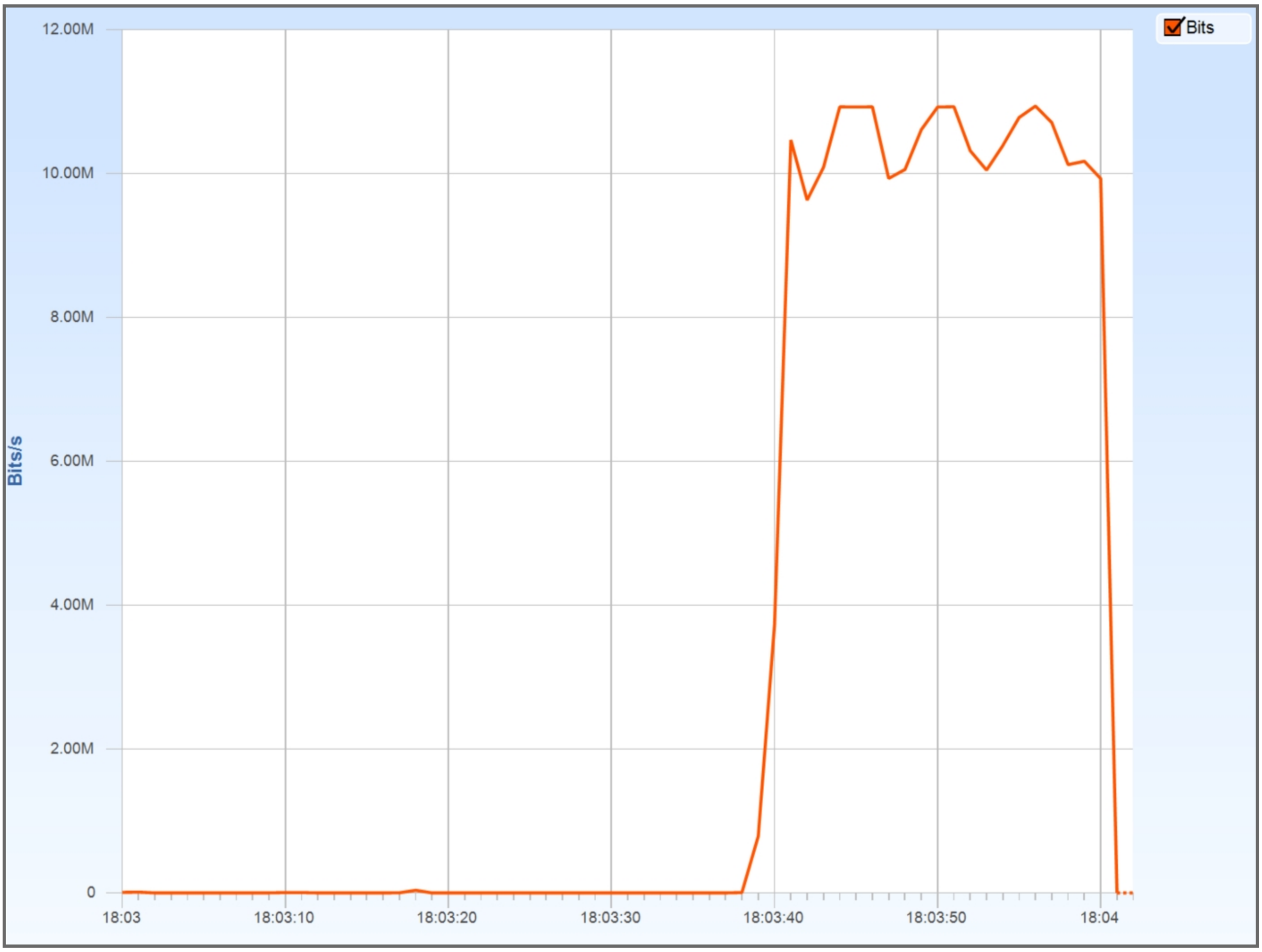

Figure 6 - Bits per Second

Packets per Second

The number of packets per second. This view when compared to the bits/bytes view above allows the user to visually identify when many small packets are generating the traffic or if it is a few larger packets.

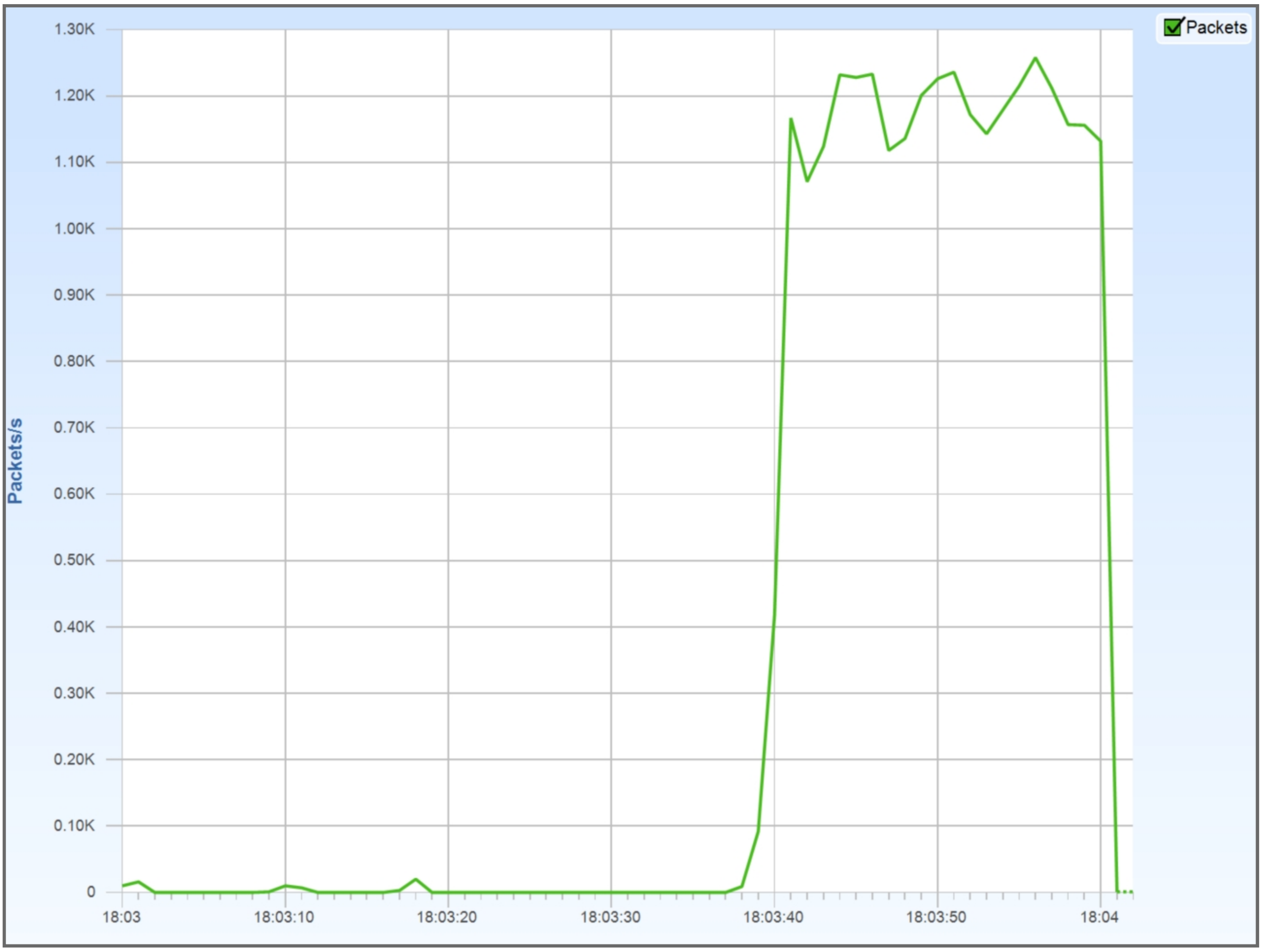

Figure 7 - Packets per Second

TCP Errors Overview

TCP Errors Overview

Applied on 1/9/2014 9:32:45 PM.

Total capture window: 11/15/2013 18:03:43.415340 - 18:04:30.415340.
Current selection: 11/15/2013 18:03:43.415340 - 18:04:30.415340 (47 s at 1 sec).

Source File: C:\Users\Laura\Documents\Customer Projects\Case 03A543\tr-twohosts.pcapng
File Time: 12/31/2013 4:03:25 PM
File Size: 54525KB
Checksum ():

Drilldown Sequence:

1. Applied the view "IP Conversations"
2. Performed a Conversation selection on the "IP Conversations" Conversation Ring. Details:
   Selected: 200.236.31.1 - 192.168.1.119
3. Applied the view "TCP Errors Overview"

TCP Errors Over Time

VIEW NOTES:
The number of TCP errors per second, charted over time.

OTHER NOTES:
This TCP Errors Overview screams that "packet loss" is the issue. Notice the pattern matches the dips in the throughput (Bandwidth Over Time) graph. Our 1.119 host is downloading a file and it appears that significant packet loss occurs during the process. Our host supports Fast Recovery (hence the Duplicate ACKs), but this cannot overcome the throughput problems caused by packet loss. We will look inside the Duplicate ACKs to see if the client is at least using SACK (119DupeACKs.pcapng). [We used the right-click | Send to Wireshark from the Total TCP Errors screen to just grab those packets.]

We also notice that there are only 454 Lost Segment indications, but over 1,000 Retransmissions. This means that we lost multiple segments in a row - complete outages rather than just single packets being dropped here and there. This is of concern since 99.99999% of the time packet loss occurs at an infrastructure device. This trace indicates that likely an infrastructure device is failing fast. We need to find out if it is one of ours and replace it asap.

NEXT STEP:
We need to capture traffic at the ingress point of our network to determine if the packet loss is occurring internally or externally. If we see the original packets AND Retransmissions in that trace file then we have a problem internally... packet loss has not occurred yet. If we only see the Retransmissions, then the problem is external to our network.

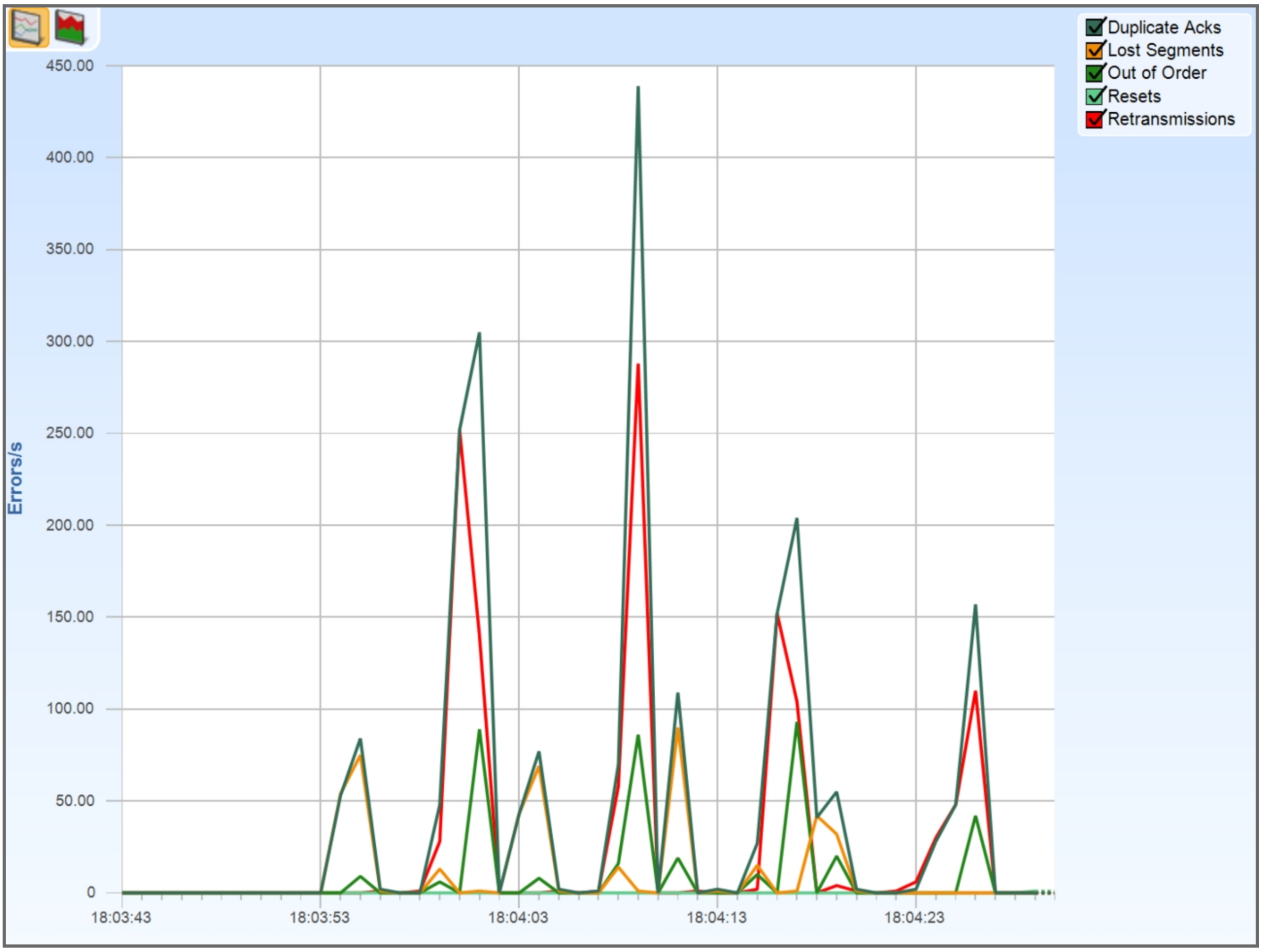

Figure 8 - TCP Errors Over Time

Relative Number of Errors

The relative number of occurrences of the different TCP errors in the period under observation.

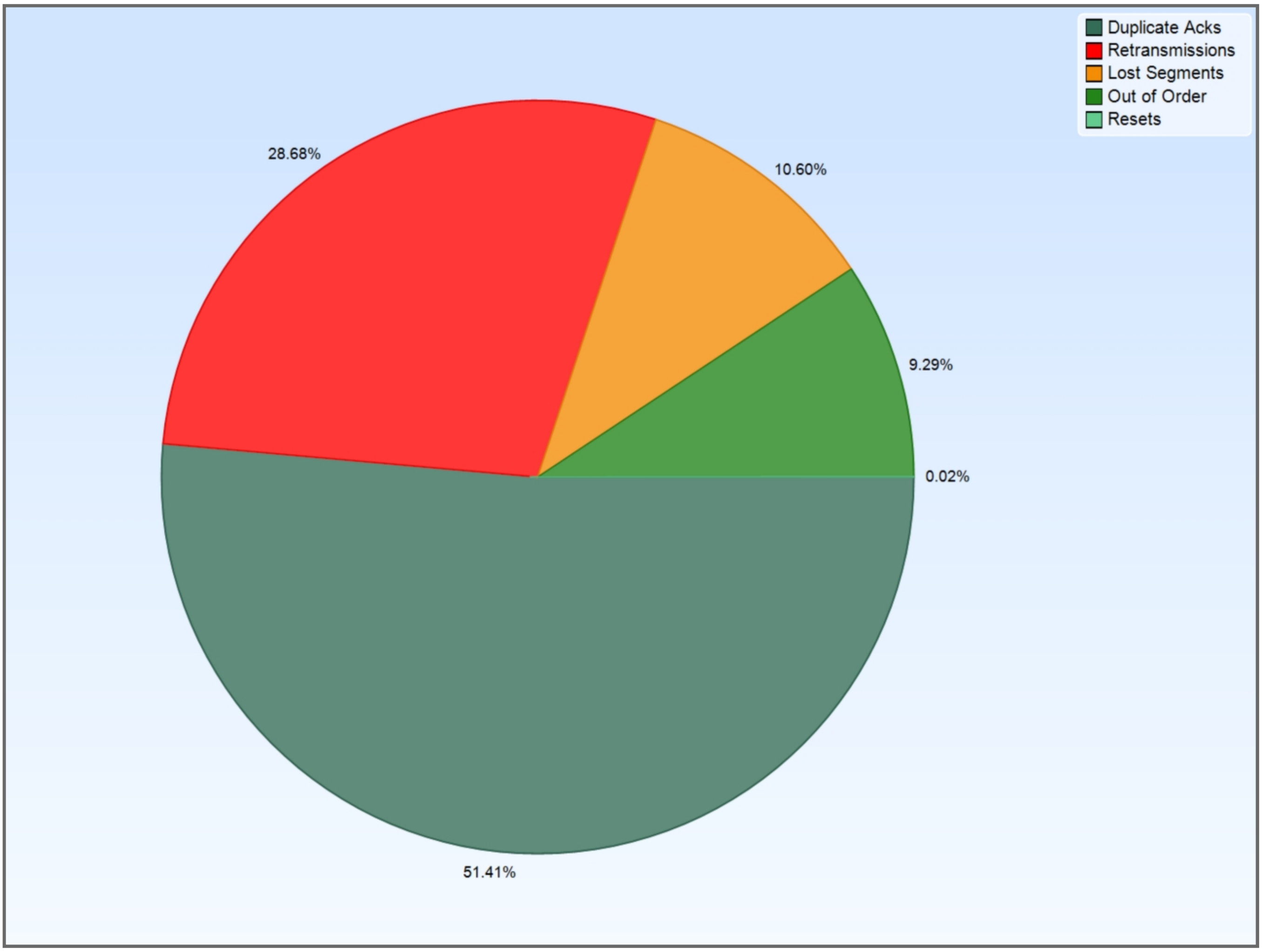

Figure 10 - Relative Number of Errors