Troubleshooting Tips and Tricks for TCP/IP Networks

June 16, 2011

Laura Chappell
Founder | Chappell University/Wireshark University
laura@chappellU.com

SHARKFEST ‘11
Stanford University
June 13-16, 2011
The “Top 10” Issues

1. Packet loss
2. Client, server and wire latency
3. Window scaling issues (RFC 1323)
4. Service response issues and application behavior
5. Network design issues (wired/wireless)
6. Path issues (such as QoS)
7. Itty Bitty Stinking Packets (Low MSS Value)
8. Fragmentation
9. Timing problems
10. Interconnecting devices
Hot Tips for TCP/IP Troubleshooting

- **Build** a troubleshooting profile*
- **Recolor** Window Update packets to green background (should not be “Bad TCP” coloring)
- **Filter** on ports, not protocols (e.g., use `tcp.port==80` rather than `http`)
- **Always** watch the time column – some networking is just ugly
- **Watch for both** Retransmissions and Fast Retransmissions in the Expert**

* See Laura’s Lab Kit v10
** as noted in the session – filter on `tcp.analysis.retransmissions` will show both standard and fast retransmissions!
Hot Tips for TCP/IP Troubleshooting

- **Recognize** a “short TCP handshake” – data is contained in the third handshake packet
- **Expand** the Conversation window to view Duration
- **Enable** TCP Conversation Timestamps (TCP protocol setting) – column?
- **Click** through the IO Graph – Don’t troubleshoot red herrings
- **Know** the definition of each TCP analysis flag
- **Watch** the handshakes!

*See Laura’s Lab Kit v10*
Your TCP/IP Troubleshooting Profile

ISO image online at lcuportal2.com
The All-Important Handshake

Focus on:
- Window Size
- Options
## TCP Options

www.iana.org/assignments/tcp-parameters/tcp-parameters.xml

<table>
<thead>
<tr>
<th>Kind</th>
<th>Length</th>
<th>Meaning</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-</td>
<td>End of Option List</td>
<td>[RFC793]</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>No-Operation</td>
<td>[RFC793]</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>Maximum Segment Size</td>
<td>[RFC793]</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>WSOPT - Window Scale</td>
<td>[RFC1323]</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>SACK Permitted</td>
<td>[RFC2018]</td>
</tr>
<tr>
<td>5</td>
<td>N</td>
<td>SACK</td>
<td>[RFC2018]</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Echo (obsoleted by option 8)</td>
<td>[RFC1072][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>Echo Reply (obsoleted by option 8)</td>
<td>[RFC1072][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>TSOPT - Time Stamp Option</td>
<td>[RFC1323]</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>Partial Order Connection Permitted (obsole)</td>
<td>[RFC1693][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>Partial Order Service Profile (obsole)</td>
<td>[RFC1693][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>CC (obsole)</td>
<td>[RFC1644][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>CC.NEW (obsole)</td>
<td>[RFC1644][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>CC.ECHO (obsole)</td>
<td>[RFC1644][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>TCP Alternate Checksum Request (obsole)</td>
<td>[RFC1146][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>15</td>
<td>N</td>
<td>TCP Alternate Checksum Data (obsole)</td>
<td>[RFC1146][RFC-eggert-tcpm-historicize-02]</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>Skeeter</td>
<td>[Stev_Knowles]</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Bubba</td>
<td>[Stev_Knowles]</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>Trailer Checksum Option</td>
<td>[Subbu_Subramaniam][Monroe_Bridges]</td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>MD5 Signature Option (obsoleted by option 29)</td>
<td>[RFC2385]</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>SCPS Capabilities</td>
<td>[Keith_Scott]</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>Selective Negative Acknowledgements</td>
<td>[Keith_Scott]</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>Record Boundaries</td>
<td>[Keith_Scott]</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>Corruption experienced</td>
<td>[Keith_Scott]</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>SNAP</td>
<td>[Vladimir_Sukonnik]</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Unassigned (released 2000-12-18)</td>
<td></td>
</tr>
</tbody>
</table>
The Ideal Handshake...

- MSS is decent size
- Window Scaling is enabled and shift factor is OK (watch out for a shift factor of 0)
- SACK is enabled
- Timestamp is on for high speed links (PAWS)
- Taken at client, the RTT is acceptable
PAWS (RFC 1323)

- Protection Against Wrapped Sequence Numbers

<table>
<thead>
<tr>
<th>Network</th>
<th>B*8 bits/sec</th>
<th>B bytes/sec</th>
<th>Twrap secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPANET</td>
<td>56kbps</td>
<td>7KBps</td>
<td>3*10^25 (~3.6 days)</td>
</tr>
<tr>
<td>DS1</td>
<td>1.5Mbps</td>
<td>190KBps</td>
<td>10^24 (~3 hours)</td>
</tr>
<tr>
<td>Ethernet</td>
<td>10Mbps</td>
<td>1.25MBps</td>
<td>1700 (~30 mins)</td>
</tr>
<tr>
<td>DS3</td>
<td>45Mbps</td>
<td>5.6MBps</td>
<td>380</td>
</tr>
<tr>
<td>FDDI</td>
<td>100Mbps</td>
<td>12.5MBps</td>
<td>170</td>
</tr>
<tr>
<td>Gigabit</td>
<td>1Gbps</td>
<td>125MBps</td>
<td>17</td>
</tr>
</tbody>
</table>
The Problem Handshake #1

Switch

Router

MSS 1460 WinScale x4 SACK

MSS 1460 WinScale x1 SACK

Mike
The Problem Handshake #1

- Ack WinSize: 500 (x4)
- WinScale x4

Uh oh... only 500 bytes receive buffer space – I’ll stop sending
The Problem Handshake #2

MSS 1460
WinScale x4
(You don’t SACK so I won’t either)

MSS 1460
WinScale x4
SACK

MSS 1460
WinScale x4

Mike

Router

Switch
Let’s Analyze a Problem

- **NAT/Firewall**
  - 10.3.8.209

- **Load Balancer**
  - 10.0.61.179

- **Mike**
  - 10.10.10.1
  - 10.3.8.109

- **10.3.8.209**

SHARKFEST ‘11 | Stanford University | June 13–16, 2011
Let’s Analyze a Problem

tcp-problem-pointA.pcap
NAT/Firewall
Load Balancer
tcp-problem-pointB.pcap
tcp-problem-pointC.pcap

Mike
Connection at Point A

SYN
- Options: 24 bytes
  - Maximum segment size: 1380 bytes
  - NOP
  - Window scale: 3 (multiply by 8)
  - NOP
  - Timestamps: TSval 184994208, TSsecr 0
  - TCP SACK Permitted Option: True
  - EOL

SYN/ACK
- Options: 8 bytes
  - Maximum segment size: 1460 bytes
  - Window scale: 0 (multiply by 1)
  - EOL
Connection at Point B

SYN
- Options: (8 bytes)
  - Maximum segment size: 1319 bytes
  - Window scale: 3 (multiply by 8)
  - EOL

SYN/ACK
- Options: (8 bytes)
  - Maximum segment size: 1460 bytes
  - NOP
  - Window scale: 8 (multiply by 256)

Mike

NAT/Firewall

Load Balancer
Connection at Point C

SYN
- Options: (8 bytes)
  - Maximum segment size: 1319 bytes
  - Window scale: 3 (multiply by 8)
  - EOL

SYN/ACK
- Options: (8 bytes)
  - Maximum segment size: 1460 bytes
  - NOP
  - Window scale: 8 (multiply by 256)
The Beliefs

- Transmission Control Protocol
  Source port: http-alt (8080)
  Destination port: 64385 (64385)
  [Stream index: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgement number: 757 (relative ack number)
  Header length: 20 bytes
  Flags: 0x10 (ACK)
  Window size: 131840 (scaled)
  Checksum: 0x5a3d [validation disabled]

My WinScale x256
131,840 bytes
The Beliefs

Transmission Control Protocol
Source port: http (80)
Destination port: 45578 (45578)
Stream index: 0
Sequence number: 1  (relative sequence number)
Acknowledgement number: 757  (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size: 515
Checksum: 0x5d1e [validation disabled]
What About this Issue?
Use Wireshark TCP Analysis Flags

• `tcp.analysis.flags`
• `tcp.analysis.lost_segment`
• `tcp.analysis.retransmission`
• `tcp.analysis.fast_retransmission`
• `tcp.analysis.duplicate_ack`
• `tcp.analysis.out_of_order`
• `tcp.analysis.window_full`
• `tcp.analysis.zero_window`
BTW: TCP Preferences Change

- Change to relative sequence numbers setting

```
Source port: ads (2550)
Destination port: http (80)
[Stream index: 0]
Sequence number: 1  (relative sequence number)
[Next sequence number: 446  (relative sequence number)]
Acknowledgement number: 1  (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size value: 64240
[Calculated window size: 256960]
[Window size scaling factor: 4]
Checksum: 0xe26a [correct]
[SEQ/ACK analysis]
(Bytes in flight: 445)
```
BTW: Using a Heuristic Dissector

- EtherType = 0800 (IP)
- IP: Type = 6 (TCP)
- TCP: Port = 80 (HTTP)
- HTTP Dissector

Hypertext Transfer Protocol

- Reassemble HTTP headers spanning multiple TCP segments: [✓]
- Reassemble HTTP bodies spanning multiple TCP segments: [✓]
- Reassemble chunked transfer-coded bodies: [✓]
- Uncompress entity bodies: [✓]

TCP Ports: 80,3128,3132,8080,8088,11371,1900

SSL/TLS Ports: 443
Questions?

laura@chappellU.com

(download the ISO of LLK10 at lcuportal.com)
Online Dating

Because crabs are filtered through the Internet