



Inside Products TCP Problem Finder

Thinking Inside the Box



www.insidestack.com

(831) 659-8360

sales@insidestack.com

Inside Products

- Products
 - Inside the Stack
 - Early Warning System
 - TCP Problem Finder
 - TCP Response Time Monitor
 - Availability Checker
 - Application Checker
 - EE Problem Finder
 - Trace Agent
 - SSL Problem Finder
 - Connection Log
- First quarter 2011
 - IPv6 Problem Finder
- Consulting
 - Network Health Check
 - EE Health Check
 - IPv6 Migration Services
- Classes
 - TCP Tuning and Performance
 - TCP Trace Analysis and Diagnostics
 - Security (IPSec, SSL)
 - IPv6 (Addressing, Migration)
 - EE Analysis



TCP Problem Finder

The product for the serious diagnostician : **TCP Problem Finder** allows you to:



- Quickly find problems in diagnostic traces - which can consist of thousands or hundreds of thousands of packets
- See the exact flow in a connection, from a high level overview to the details .



```
758 HOST1      PACKET      00000001 07:50:10.150761 Packet Trace
To Interface   : GBE1                Device: QDIO Ethernet      Full=60
Tod Clock      : 2009/12/03 07:50:10.150761
Sequence #     : 0                Flags: Pkt Ver2 Out
Source Port    : 5023             Dest Port: 3886  Asid: 0066 TCB: 00000000
IpHeader: Version : 4                Header Length: 20
Tos            : 00                QOS: Routine Normal Service
Packet Length  : 60                ID Number: F585
Fragment       :                    Offset: 0
TTL            : 64                Protocol: TCP                CheckSum: E4BA
Source         : xxx.194.129.241
Destination    : xxx.194.129.5
```

Typical trace packet. It is hard for even experienced analysts to find problems .

TCP

```
Source Port    : 5023  ( )          Destination Port: 3886  ( )
Sequence Number : 1441719441      Ack Number: 3392023215
Header Length   : 40              Flags: Ack Syn
Window Size     : 65535           CheckSum: 4AD2 FFFF      Urgent Data: 0000
Option         : Max Seg Size Len: 4 MSS: 1460
Option         : NOP
Option         : Window Scale OPT Len: 3 Shift: 0
Option         : NOP
Option         : NOP
Option         : Timestamp        Len: 10 Value: DA182CA7 Echo: DA182CA6
```

What Happened?

Drill Down	Total Occurrences by Error Code	Error Code	Error Code Decoded
	124	100	<p>This is most likely an unrecoverable error. No data was received from partner. Data traffic was received from the source IP address and source port but not the destination IP address and port. The destination server may not have a listening port at the port indicated, there may be a firewall issue or the data traffic from the source IP and port may be inappropriate overhead.</p>
	2	101	<p>This is an unrecoverable error. Bad TCP Open (RST). A TCP Open (SYN) packet was sent from the source IP address and source port to start a session with the application at the destination port. The destination IP address and port responded with a RESET packet rather than the SYN-ACK packet which was expected. Reasons for this include:</p> <ul style="list-style-type: none">• The destination server may not have a listening port at the port indicated.• The destination server may have capacity issues or

- TCP Problem Finder will tell you what kind of errors were found in the trace and how many time.

Where Did It Happen?

Error Code : 121

This error is a performance warning. Small window sizes were found in the data traffic. Receive congestion window sizes which are less than 10,000 were found. This may cause performance degradation. Data traffic is transferred but it may be slower than desired or possible.

- Destination Port
 - Destination port 515 is responsible for 73.33% of the total errors.
- Source IP
 - 10.120.10.216 is responsible for 73.33% of the total errors.
- Source Network (Octet1 - Octet3)
 - 10.120.10 is responsible for 86.66% of the total errors.
- Source Network (Octet1)
 - 10 is responsible for 100.0% of the total errors.
- Destination Network (Octet1)
 - 10 is responsible for 100.0% of the total errors.

- Next, you probably want to know where exactly the problems were.

Session Details

- No small window sizes from 10.236.78.103:1119 were found in the data flow.
- No zero window sizes from 10.120.10.200:23 were found in the data flow.
- No zero window sizes from 10.236.78.103:1119 were found in the data flow.

Duplicate Segments

- No duplicate segments from 10.120.10.200:23 were found in the data flow.
- Duplicate segments were found on this session from 10.236.78.103:1119.
- The number of duplicate segments received is: 1. The total packets received is: 5. The percent of packets which are duplicate segments is:20.0%.
- The number of bytes received in duplicate segments is: 14. The total bytes received is: 28. The percent of bytes received in duplicate segments is:50.0%.
- Packet 1318992 was duplicated 1 times.

10.120.10.200:23
10.236.78.103:1119

- You may want to analyze exactly what happened in the session.
- From the TCP open to data transmission to the close is analyzed for problems.

View Data as 3270 Screen

```
----- ISO/E LOGON -----
|
| Enter LOGON parameters below:                                RACF LOGON parameters:
|
| Userid   ===> ██████████                                     Seclabel   ===>
|
| Password ===>                                              New Password ===>
|
| Procedure ===> ██████████                                   Group Ident ===>
|
| Acct Nmbr ===> ██████████
|
| Size     ===> 32768
|
| Perform  ===>
|
| Command  ===>
|
| Enter an 'S' before each option desired below:
|      -Nomail          -Nonotice          -Reconnect          -OIDcard
|
| PF1/PF13 ==> Help    PF3/PF15 ==> Logoff   PA1 ==> Attention   PA2 ==> Reshow
| You may request specific help information by entering a '?' in any entry field
|
|-----
```

- Diagnostics can be much easier if you can see the screen the way the user saw it.

TCP Response Time Monitor

The screenshot displays the website for the Department of Buildings. At the top, there is a navigation bar with links for "Residents", "Business", "Visitors", and "Government". A search bar and "Email Updates" and "Contact Us" links are also present. The main header features the "BUILDINGS" logo and the text "DEPARTMENT OF BUILDINGS". A "SIGN UP FOR BUILDINGS NEWS" button is located on the right side of the header. The main content area is titled "BUILDINGS INFORMATION SYSTEM" and includes a large blue button labeled "ENTER BUILDINGS INFORMATION SYSTEM". Below this button, a paragraph describes the BIS as the Department's main database, established in 1984. On the right side, there is a "BIS WEB QUERY" section with input fields for "HOUSE #" and "STREET NAME", and "SUBMIT" and "CLEAR" buttons. A left sidebar contains a search bar, a "SEARCH BUILDINGS DEPT" button, and a menu with links to "HOME", "ABOUT THE BUILDINGS DEPT", and "BUILDINGS INFORMATION SYSTEM (BIS)", which includes sub-links for "BIS FAQ" and "BIS Glossary". The background of the main content area features a blue-tinted architectural floor plan with labels like "COPY STORAGE" and "OFFICE".

Critical application used over the Internet was experiencing intermittent response time problems. Unclear if the problem is in the network, the z/OS host, the application or Linux. Here is how TCP Response Time Monitor allowed the customer to solve the problem.

Response Time Breakout

-	Transaction Date	Interface	Device	Source Address	Source Port	Destination Address	Destination Port	End-To-End Time (MS)	Host Time (MS)	Network Time (MS)
1	2007-02-06 13:24:08.362809	OSAELNK1	QDIO		.42 50492		.65 4001	18,909	18,908	1
2	2007-02-06 13:23:58.201494	OSAELNK1	QDIO		.42 50477		.65 4001	17,082	17,081	1
3	2007-02-06 13:23:42.127722	OSAELNK1	QDIO		.42 50469		.65 4001	16,048	16,047	1
4	2007-02-06 13:23:42.221918	OSAELNK1	QDIO		.42 50470		.65 4001	15,970	15,968	1

- Customer was not able to solve problem for 2 months. With TCP Response Time Monitor, they solved it in 2 days.
- See above a sample trace analyzed by the TCP Response Time Monitor product.
- Found that z/OS mainframe times were quite long at times when people were experiencing problems.
- Network time, which included the zLinux, is negligible.

EE Problem Finder

Total Number of Packets	Total Number SNA Packets with Productive RU Data	Total Number Packets ARB Pacing or Status Only *	Total Number Packets XID Test Only *	Total Number Packets XID Negotiation *	Total Number Packets Isolated Pacing Messages *	Total Number of SNA THRH Only Packets *	Total Number Packets Data Flow Or Session Control Messages *
11,905	5K (46.25%)	4K (39.08%)	0 (0.0%)	0 (0.0%)	373 (3.13%)	1K (9.4%)	204 (1.71%)

Some of the things we want to know:

- Are we sending packets unnecessarily?
- Do we have routing loops?
- If we have such data, what kind and how do we do something about it?

Total Number RTP Pipes	Total Number RTP Pipes No SNA Productive Packets
635	330

Notice in the statistics:

- Fairly low percentage of productive packets
- Low number of RTP pipes with productive packets
- Many ARB flow packets

Why is EE Analysis Hard?

- Enterprise Extender uses HPR/RTP within IP/UDP.
- To find problem, we have to decode multiple headers.
- Inside some of the headers are indicators of congestion or problems
- RTP will retransmit data, if needed, so control information for retransmission is in some of the headers.
- RTP will try to adapt to changing network conditions, so some headers contain information needed for flow control.

EE Packet Headers

IP Header (20 bytes)

UDP Header (8 bytes)

LLC Header (3 bytes)

NLC (variable)

RTP Header (20 bytes)

Optional RTP Segments

FID5 TH

RH (3 bytes)

RU – SNA Data

Errors / Congestion Control

Errors

Total Number Packets Gap (Retransmission) Indicators *	Total Number Packets HPR Fragments *	Total Number Packets SNA Fragments *
0 (0.0%)	1K (14.88%)	1K (15.9%)

Congestion Control

Total Number Packets Slowdown 1 *	Total Number Packets Slowdown 2 *	Total Number Packets Critical *
1 (0.0%)	21 (0.17%)	0 (0.0%)

We want to know error information:

- Do we have retransmissions?
- Is fragmentation done?
- If we have such data, what kind and how do we do something about it?

We want to know flow control information:

- Do we have slowdowns?
- Who is doing it?
- If we have such data, what kind and how do we do something about it?

We analyze the trace and provide a summary.
You can drill down to the details.

Show EE Log

Sort Order : Packet Number

Showing Entries : 1 -10

Trace File:earbs2

We provide a flow of events with warnings and alerts.

	Packet Number	Identifier	RTP	ANRLLabels	Warnings
3	153619	Address: [redacted] Source Port: 12002 Destination Address: [redacted] Destination Port: 12002 DSAP: 04 SSAP: 08	RTP: TCID: 1B0AFC7000011ED8 RTP: Start of User Data RTP: End of User Data RTP: Status Requested RTP: Respond ASAP RTP: Optional Segments Present RTP: SNA Data: 195 RTP: Byte Sequence Number: 04567320 RTP: ARB Pacing: MessageType: Rate Request RTP: ARB Pacing: Parity: 0 RTP: ARB Pacing: ARBMode: Responsive RTP: ARB Pacing: RateRequestCorrelator: 3 RTP: ARB Pacing: RateReplyCorrelator: 0 RTP: ARB Pacing: Field1: 1685392	NLP: SwitchingMode: 110 NLP: Transmission Priority: 10 NLP: TimeSensitive: 1 D000000000000000	RTP: ARB Pacing: Parity: 0 - Replies not received
4	153622	2005-08-03 12:59:44.045343 Interface: LOSA4 Device: QDIO Source Address: [redacted] Source Port: 12003 Destination Address: [redacted] Destination Port: 12003 DSAP: 04 SSAP: 08	RTP: TCID: 096B398600000476 RTP: Optional Segments Present RTP: SNA Data: 0 RTP: Byte Sequence Number: 1679BBF1 RTP: ARB Pacing: MessageType: Rate Reply RTP: ARB Pacing: RateAdjustment: Slowdown2 RTP: ARB Pacing: Parity: 0 RTP: ARB Pacing: ARBMode: Responsive RTP: ARB Pacing: RateRequestCorrelator: 0 RTP: ARB Pacing: RateReplyCorrelator: 10 RTP: ARB Pacing: Field1: 0	NLP: SwitchingMode: 110 NLP: Transmission Priority: 10 NLP: TimeSensitive: 1 801A003601000000 D000000000000000	RTP: ARB Pacing: RateAdjustment: Slowdown2