TCP Analytics

(Optimized TCP Record Processing)



Overview

GL's TCP Analytics application analyzes TCP connections between both internal Local Area Network (LAN) and external Wide Area Network (WAN) computers including servers and clients. The application helps troubleshoot large bandwidth consumption, failed TCP sessions, packet loss, poor TCP throughput and more. TCP Analytics (PKV400) is an optional application with <u>PacketScan[™] All IP</u> protocol analysis software.

The core functionality is based on the data structures created by sequential processing of the TCP segments in the offline trace file of the PacketScan[™]. Due to the requirement to process huge trace files with billions of records the TCP Analytics is not based on the protocol decode functions but rather on the optimized fast TCP record processing.

These data structures need to be created once when the offline trace file is opened and are used to produce derivatives analytics. When offline file is closed the data structures are destroyed releasing memory resources.

PacketScan[™] offline user interface is used to create base data structures for TCP connection analysis from an offline trace file containing captured frames or importing Wireshark packet captures. These data structures could be huge if the captured data files are hundreds of gigabytes or even many terabytes (1OE+12) in size. The proper configuration of computer's virtual memory is required to handle this data and is accomplished with the TCP Analytics program.

For more details, refer to <u>TCP Analytics</u> webpage.



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A (Web) <u>www.gl.com</u> - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) <u>info@gl.com</u>

Main Features

- Analyze TCP connections between internal company LAN connected computers and outside computers on the WAN
- Analyze TCP connections of a particular client server pair
- Analyze TCP connections on a subset of a LAN
- Display top level statistics
- Use PacketScan[™] to display packets that belong to a selected TCP connection
- Export information to CSV files for subsequent Excel or a database import
- Sort tabular information by column values

TCP Analytics GUI (TAG) IPv4 Dashboard

The TAG dashboard includes a menu to invoke detailed TCP IPv4 connection information and summary overview of TCP connections in the currently opened and processed trace file. The window is resizable to adjust column width. Columns can be sorted by clicking on the column header.

TCP II	Pv4 Analytics							
Serv	ver Client							
otal TC	P Connection Info			Closed, Open, Orphan	Connections %		Top Servers not Accepting Conne	tions (3+ conn)
A 11 - 1		<u> </u>						T
Attribu	ute	Count		Attribute	%	1~	IP Addr Port %RS	I lotC /
Bytes		19,450,107,544		ClosCon Bytes	73.841285		1.1.2.55 7,680 100.0	00000 287
Packet	s	73,526,636		OpenCon Bytes	7.105502		3.33.141.226 443 100.0	00000 3
Conne	ctions	833,748		OrphCon Bytes	19.053213		3.85.155.49 443 100.0	00000 22
Seq Er	rrors	9,786,559		ClosCon Packets	29.068371		3.91.163.71 443 100.0	00000 8
Resets	5	254,785		OpenCon Packets	20.506562		3.209.40.129 443 100.0	00000 4
Conge	stions	6,511,737		OrphCon Packets	50.425068		3.210.69.174 443 100.0	00000 8
Severe	e Cong	7,906,264		ClosCon ServIp	0.321143		3.221.115.1 443 100.0	100000 4
Serv I	Ps	1,443,907		OpenCon Servip	99.61/496		3.226.32.236 443 100.0	100000 4
Client	IPS	38,961		OrphCon Servip	0.363458		3.228.31.194 443 100.0	00000 6
				ClosCon ClientIp	7.5/93/4	\sim	3.233.68.37 443 100.0	100000 4
				<	>			>
				1				
IP Add	ir Port	TotBytes		TP Addr Port	%Cong		TP Addr Port %	SegErr
IP Add	dr Port	TotBytes	<u>_</u>	IP Addr Port	%Cong	<u>_</u>	IP Addr Port %	SeqErr
34.104	1.35.123 80	1,561,515,		192.168.1.0 22	100.000000		192.168.30 3,389 9	9.760066
38.127	7.147.51 443	1,169,750,		192.168.1.0 5,432	100.000000		27.59.27.230 3,207 9	9.709302
209.19	97.3.8 80	890,596,282		192.168.1.0 6,379	100.000000		27.59.27.230 2,878 9	9.604743
108.31	1.185 4,433	536,250,238		192.168.1.0 8,500	100.000000		27.59.27.230 3,201 9	9.601594
/2.21.	81.240 80	504,950,907		192.168.1.1 22	100.000000		27.59.27.230 2,865 9	1.59/586
8.253.	254.120 80	4/4,039,204		192.168.1.1 5,432	100.000000		27.59.27.230 3,180 9	3.505217
8.253.	45.249 80	404,317,774		192.108.1.1 8,500	100.000000		27.59.27.230 2,900 9	9.415205
23.38.	167.136 80	310,338,404		192.168.1.2 22	100.000000		106.51.67.50 2,804 9	3.337748
72.21.	91.29 80	309,212,339		192.108.1.2 5,432	100.000000		27.59.27.230 3,024 9	9.120038
23.00.	159.42 80	303,873,305		192.108.1.2 0,379	100.000000		192.108.30.04 3,389 9	9.02/030
22.20.	107.100 00	277 464 420	\sim	192.100.1.2 0,500	100.000000	\sim	27.59.27.250 3,215 9	0 004701
/ 100		777 414 4 31		1147 108 1 3 77		_		1 004701
ор ТСР	Applications by By	/tes		Top Clients by Bytes			Top Clients by Packets	
ort	Application	TotBytes	^	IP Addr	Tot Bytes	^	IP Addr Tot Pack	ets 🗖
0	World Wide W	7,714,692,228		108.31.185.150	5,065,572,127		192.168.31.17 11,927,1	79
43	http protocol o	5,698,076,260		50.76.16.177	3,815,217,823		192.168.30.128 10,462,5	76
2	The Secure S	2,994,573,217		192.168.31.17	1,046,328,921		192.168.31.49 6,882,77	6
,433	Versile Object	536,421,433		192.168.30.128	960,444,741		108.31.185.150 6,549,68	3
,680	Pando Media P	257,791,734		192.168.10.24	682,603,180		50.76.16.177 5,127,30	2
,389	Adept IP proto	216,431,913		192.168.31.49	676,152,727		192.168.30.180 4,170,87	0
,832	silkp4	107,558,876		192.168.10.67	585,411,221		151.196.118.90 1,075,78	0
,831	silkp3	105,640,248		192.168.10.111	378,489,782		192.168.10.24 995,025	
45	Microsoft-DS	102,961,709		192.168.10.100	357,931,100		192.168.10.149 857,659	
87	Message Sub	91,702,667		192.168.30.180	311,789,672	~	192.168.10.67 691,065	
,947	SentinelSRM	46,231,897		100 100 10 104	200 027 120	Ť	70 00 14 01 0007	
			~		>			>

TAG IPv4 Dashboard

🌑 GL Communications Inc.

Sorting Columns

Sort columns in an ascending or descending order.

IP Addr	Port	TotBytes	^
8.240.25.126	80	54,548,403	
8.240.241.254	80	28,162,715	
8.248.153.254	80	31,738,911	
8.248.163.254	80	34,703,316	
8.248.165.254	80	31,573,754	
8.249.217.254	80	82,444,913	
8.249.241.254	80	37,579,056	
8.250.89.254	80	37,467,570	
8.252.11.126	80	30,300,605	
8.252.64.254	80	57,775,742	
8.252.65.254	80	28,338,810	
8.252.81.126	80	83,224,445	
8.253.45.249	80	464,317,774	
8 253 156 121	80	47 077 077	~

Sorting Columns

Total TCP Connection Information

- Seq Errors for TCP Sequence Number field errors indicate missing, duplicate or out of order packets
- Resets are connections with RST flags usually indicates refused connections by servers etc.
- Congestions indicate reduced window size due to congestions (indication of the receiving side to slow down transmission on the other end)
- Severe Cong indicates 0 window size in the TCP header when receiving size cannot accept ANY TCP packets for the connection
- Serv IPs, Client IPs just counts the unique IPv4 addresses for servers and clients

Attribute	Count
Bytes	19,450,107,544
Packets	73,526,636
Connections	833,748
Seq Errors	9,786,559
Resets	254,785
Congestions	6,511,737
Severe Cong	7,906,264
Serv IPs	1,443,907
Client IPs	38,961

Total TCP Connection Information

🌑 GL Communications Inc.

Distribution in Percentage Among Closed, Open and Orphan Connections

Display Closed, Open, and Orphan connections in percentage.

Attribute	%	^
ClosCon Bytes	73.841285	
OpenCon Bytes	7.105502	
OrphCon Bytes	19.053213	
ClosCon Packets	29.068371	
OpenCon Packets	20.506562	
OrphCon Packets	50.425068	
ClosCon ServIp	0.321143	
OpenCon ServIp	99.617496	
OrphCon ServIp	0.363458	
ClosCon ClientIp	7.579374	
0C ClIT-	00 570005	, i

Closed, Open, and Orphan Connections

Top Servers Rejecting Client Connections

- IP Addr and Port columns display server IP address and TCP port number
- %RST (resets) is the percentage of connections being rejected. This list includes only servers with total of 3 or more connections to avoid noise
- TotCon is the total number of connections to the server addr/port pair

IP Addr	Port	%RST	TotCon	^
38.127.147.51	443	100.000000	1,420	
38.127.147.80	443	100.000000	788	
13.68.20.25	443	100.000000	691	
1.1.2.55	7,680	100.000000	287	
13.107.6.158	443	100.000000	230	
20.49.104.34	443	100.000000	107	
40.70.184.83	443	100.000000	102	
13.83.65.43	443	100.000000	98	
20.110.132	443	100.000000	98	
13.107.21.200	443	100.000000	96	5
00.04.100	440	100.000000	76	

Top Servers Rejecting Client Connections

GL Communications Inc.

Top Servers by Bytes Transferred

Information is collected only for connections with 5 or more segments for a connection. Each line is a total for all connections for a particular server TCP application with unique IP address and TCP port.

IP Addr	Port	TotBytes	1
192.168.12.60	22	205,538,848	
192.168.12.97	22	177,176,032	
192.168.12.199	22	147,317,710	
192.168.12.239	22	199,540,974	
192.168.15.121	22	205,982,088	
8.240.25.126	80	54,548,403	
8.240.241.254	80	28,162,715	
8.248.153.254	80	31,738,911	
8.248.163.254	80	34,703,316	
8.248.165.254	80	31,573,754	
0.040.017.054	00	02 444 012	

Top Servers by Bytes Transferred

Top Servers with Reduced Windows Size (Congested)

Includes connection with at least 5 segments (packets) and is showing servers with the largest percentage of packets with reduced window size.

IP Addr	Port	%Cong	^
192.168.1.0	22	100.000000	
192.168.1.0	5,432	100.000000	
192.168.1.0	6,379	100.000000	
192.168.1.0	8,500	100.000000	
192.168.1.1	22	100.000000	
192.168.1.1	5,432	100.000000	
192.168.1.1	8,500	100.000000	
192.168.1.2	22	100.000000	
192.168.1.2	5,432	100.000000	
192.168.1.2	6,379	100.000000	
100 100 1 0	0.500	100.000000	· · ·

Top Servers with Reduced Window Size



Top Servers with Largest Percentage of Sequence Errors (Packet Loss/Retransmission)

Indicates the most affected servers by percentage of TCP segments with sequence number errors caused by missed packets, packets retransmission and reordering etc.

op Servers with	Packet Loss/Retra	nsm (5+ segm)-	
IP Addr	Port	%SeqErr	^
192.168.30.124	3,389	99.760066	
27.59.27.230	3,207	99.709302	
27.59.27.230	2,878	99.604743	
27.59.27.230	3,201	99.601594	
27.59.27.230	2,865	99.597586	
27.59.27.230	3,180	99.565217	
27.59.27.230	2,900	99.415205	
106.51.67.50	2,804	99.337748	
27.59.27.230	3,024	99.126638	
192.168.30.64	3,389	99.027650	
27.59.27.230	3,215	99.014778	
27 59 27 230	3 223	98 804781	~

Top Servers with Packet Loss or Retransmission

Top TCP Applications by Received Bytes

Total bytes are the sum of all bytes for all connections to all IP addresses with particular TCP port number.

Port	Application	TotBytes	\mathbf{h}
80	World Wide Web HTTP	7,714,692,228	
443	http protocol over TLS/SSL	5,698,076,260	
22	The Secure Shell (SSH)	2,994,573,217	
4,433	Versile Object Protocol	536,421,433	
7,680	Pando Media Public	257,791,734	
3,389	Adept IP protocol	216,431,913	
2,832	silkp4	107,558,876	
2,831	silkp3	105,640,248	
445	Microsoft-DS	102,961,709	
587	Message Submission	91,702,667	5
<	CP JODM	<pre>// 007</pre>	Ť

Top TCP Applications by Received Bytes



Top Client IP Addresses by Bytes for all Client TCP Connections

- Used to diagnose computers that cause the network congestions
- These are the clients that transmit or receive largest amount of data
- This is a total for all connections and all TCP applications per client

IP Addr	Tot Bytes	^
108.31.185.150	5,065,572,127	
50.76.16.177	3,815,217,823	
192.168.31.17	1,046,328,921	
192.168.30.128	960,444,741	
192.168.10.24	682,603,180	
192.168.31.49	676,152,727	
192.168.10.67	585,411,221	
192.168.10.111	378,489,782	
192.168.10.100	357,931,100	
192.168.30.180	311,789,672	5
100 100 10 104	200 027 120	Ť
<	>	



Top Client IP Addresses by Packets for all Client TCP Connections

- Total for all connections and all TCP applications per client
- Used to diagnose computers that cause the network congestions and potential viruses or wiring and Hardware malfunctions
- These are the clients that transmit or receive largest number of packets

IP Addr	Tot Packets	^
192.168.31.17	11,927,179	
192.168.30.128	10,462,576	
192.168.31.49	6,882,776	
108.31.185.150	6,549,683	
50.76.16.177	5,127,302	
192.168.30.180	4,170,870	
151.196.118.90	1,075,780	
192.168.10.24	995,025	
192.168.10.149	857,659	
192.168.10.67	691,065	
72.83.14.31	679,037	
192 168 10 100	504 721	~

Top Client IP Address by Packets for all Client TCP Connections



TAG IPv6 Dashboard

The TAG dashboard includes a menu to invoke detailed TCP IPv6 connection information and summary overview of TCP connections in the currently opened and processed trace file. The window is resizable to adjust column width. Columns can be sorted by clicking on the column header .

Attribute										
	Count		Attribute	%		^	IP Addr	Port	%RST	Tot
vtes	49,112		ClosCon Bytes	97.923115			fe80::50a:23a2:708e:9ad6	5,357	0.000000	4
ackets	148		OpenCon Bytes	0.586415			fe80::21d6:cd0f:1d68:e0b4	5,357	0.000000	8
Connections	24		OrphCon Bytes	1.490471						
eq Errors	0		ClosCon Packets	89.189189						
esets	0		OpenCon Packets	2.702703						
Congestions	0		OrphCon Packets	8.108108						
evere Cong	0		ClosCon ServIp	66.666667						
erv IPs	3		OpenCon ServIp	33.333333						
lient IPs	2		OrphCon ServIp	66.666667						
			ClosCon ClientIp	50.000000						
			0	50 000000		*				
Servers by Bytes (5+ se	gm)		Top Servers with Conge	estion (5+ segm)	>		Top Servers with Packet Loss/	Retransm	(5+ segm)	
P Addr	gm)	TotBytes	Top Servers with Conge	estion (5+ segm) Port	> %Cong		Top Servers with Packet Loss/I	Retransm	(5+ segm)	
o Servers by Bytes (5+ se P Addr e80::21d6:cd0f:1d68:e0b- e80::50a:23a2:708e:9ad6	gm) Port 4 5,357 5 357	TotBytes 32,544 16,268	Top Servers with Conge IP Addr fe80::50a:23a2:7 fe80::21d6:cddf:1	estion (5+ segm) Port 5,357 5 357	> %Cong 0.000000 0.000000		Top Servers with Packet Loss// IP Addr fe80::50a:23a2:708e:9ad6 fe80::21dc:rd0f:168::e0b4	Retransm	(5+ segm) Port 5,357 5 357	
o Servers by Bytes (5+ se P Addr 180::21d6:cd0f:1d68:e0b 1800::50a:23a2:708e:9ad6	gm) Port 4 5,357 5,357	TotBytes 32,544 16,268	Top Servers with Conge IP Addr fe80::50a:23a2:7 fe80::21d6:cd0f:1	estion (5+ segm) Port 5,357 5,357	> %Cong 0.000000 0.000000		Top Servers with Packet Loss/I IP Addr fe80::50a:23a2:708e:9ad6 fe80::21d6:cd0f:1d68:e0b4	Retransm	(5+ segm) Port 5,357 5,357	
o Servers by Bytes (5+ ser P Addr 880::21d6:cd0f:1d68:e0b 880::50a:23a2:708e:9ad6	gm) Port 4 5,357 5,357 5,357	TotBytes 32,544 16,268	Top Servers with Conge IP Addr fe80::50a:23a2:7 fe80::21d6:cd0f:1	estion (5+ segm) Port 5,357 5,357	> %Cong 0.000000 0.000000	>	Top Servers with Packet Loss/I IP Addr fe80::50a:23a2:708e:9ad6 fe80::21d6:cd0f:1d68:e0b4 <	Retransm	(5+ segm) Port 5,357 5,357	
o Servers by Bytes (5+ ser P Addr 280::21d6:cd0f:1d68:e0b 280::50a:23a2:708e:9ad6 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005 - 2005	gm) Port 4 5,357 5,357 5,357	TotBytes 32,544 16,268	Top Servers with Conge IP Addr fe80::50a:23a2:7 fe80::21d6:cd0f:1 < Top Clients by Bytes	estion (5+ segm) Port 5,357 5,357	> %Cong 0.000000 0.000000	>	Top Servers with Packet Loss/I IP Addr fe80::50a:23a2:708e:9ad6 fe80::21d6:cd0f:1d68:e0b4 Top Clients by Packets	Retransm	(5+ segm) Port 5,357 5,357	
o Servers by Bytes (5+ sep P Addr 180::21d6:cd0f:1d68:e0b- 180::50a:23a2:708e:9ad6 100 CP Applications by Byte rt Applic	gm) Port 4 5,357 5,357 5,357 15 25 25 25 25 25 25 25 25 25 2	TotBytes 32,544 16,268	Top Servers with Conge IP Addr fe80::50a:23a2:7 fe80::21d6:cd0f:1 < Top Clients by Bytes IP Addr	estion (5+ segm)	> %Cong 0.000000 0.000000	>	Top Servers with Packet Loss/I IP Addr fe80::50a:23a2:708e:9ad6 fe80::21d6:cd0f:1d68:e0b4 Top Clients by Packets IP Addr	Retransm	(5+ segm) Port 5,357 5,357 ckets	

TAG IPv6 Dashboard



Buyer's Guide

ltem No	Product Description
<u>PKV400</u>	TCP Analytics (Optional with PacketScan™)
Item No	Related Software
<u>PKV100</u>	PacketScan [™] - (Online and Offline)
<u>PKV101</u>	Offline PacketScan™
Item No	Related Hardware
<u>PKV120</u>	PacketScan™ HD High Density IP Traffic Analyzer

<u>Note</u>: PCs which include GL hardware/software require Intel or AMD processors for compliance.

For more details, refer to <u>TCP Analytics</u> webpage.



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A (Web) <u>www.gl.com</u> - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) <u>info@gl.com</u>