TcpAnalyzer

Windows TCP Analyzer

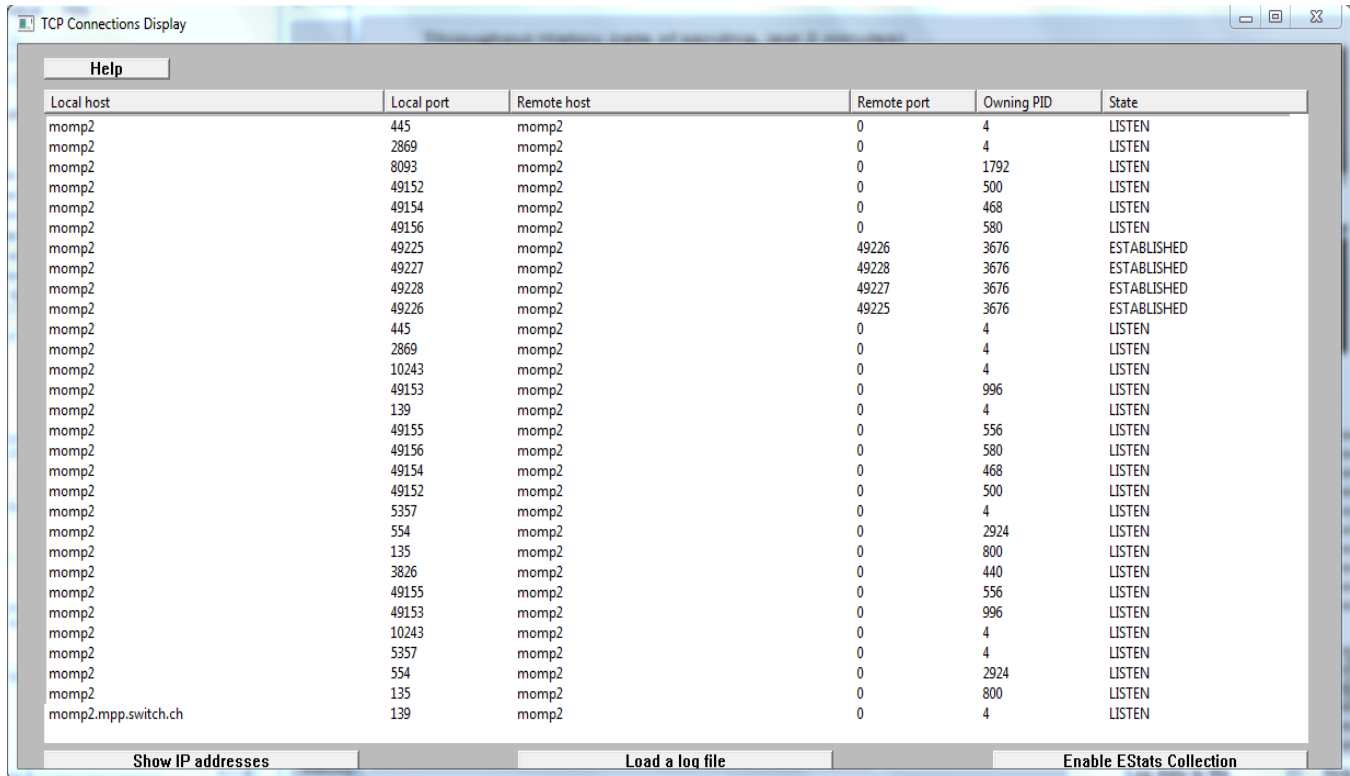The Microsoft Windows SDK also contains a tool that can read the so called ESTATS of an open TCP connection.
When running, you get a listing of all current TCP connections. Then you can click on one and see statistics about it in a new window. You can get a throughput history, find out where most time is spent during the connection. This is good to find out performance bottlenecks of an already running application, without interrupting it.
Unfortunately to install this tool you need to download and install the whole SDK (the ISO image is a whopping 1.3GB), as there is no separate installation available.
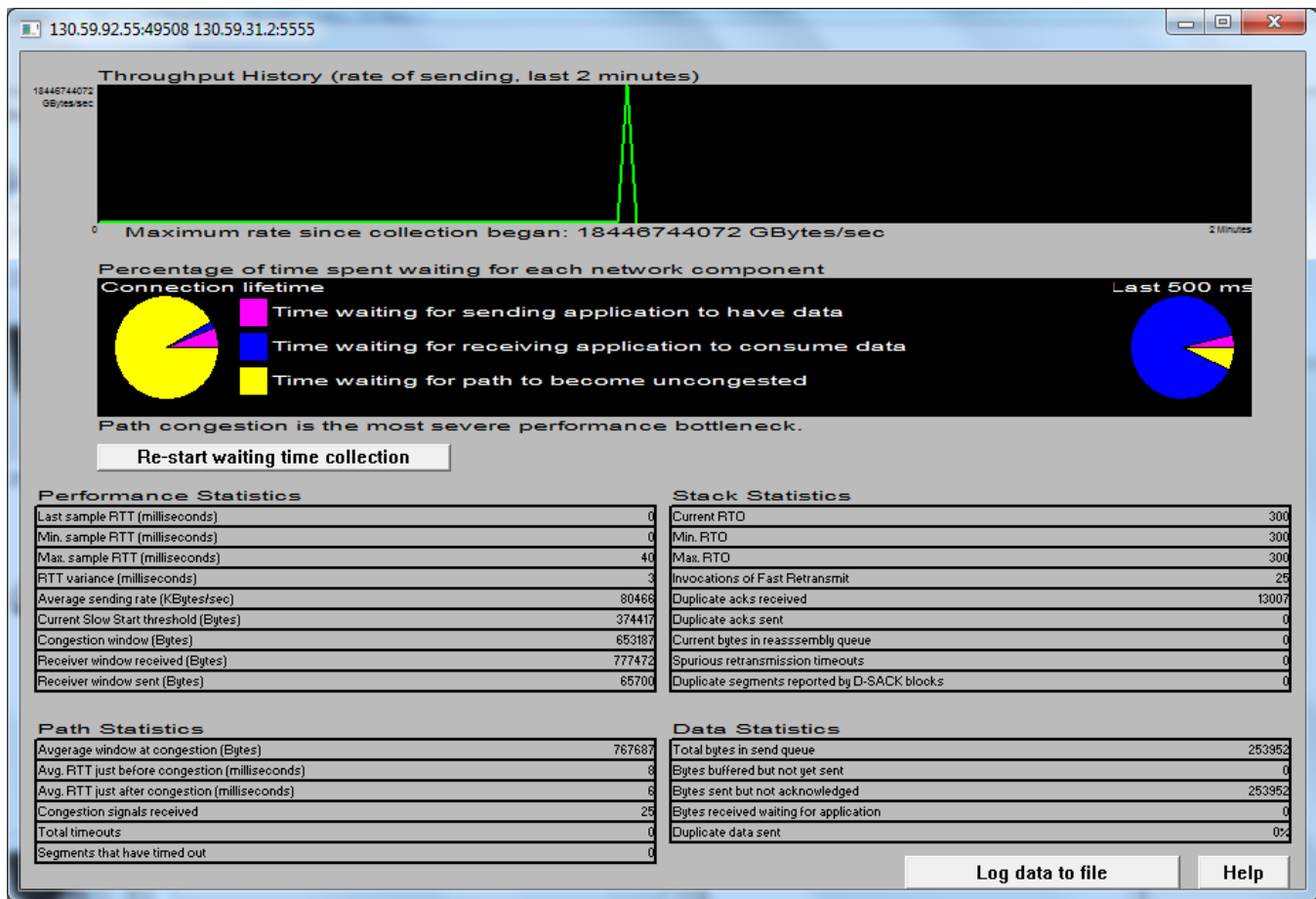More information is available here.
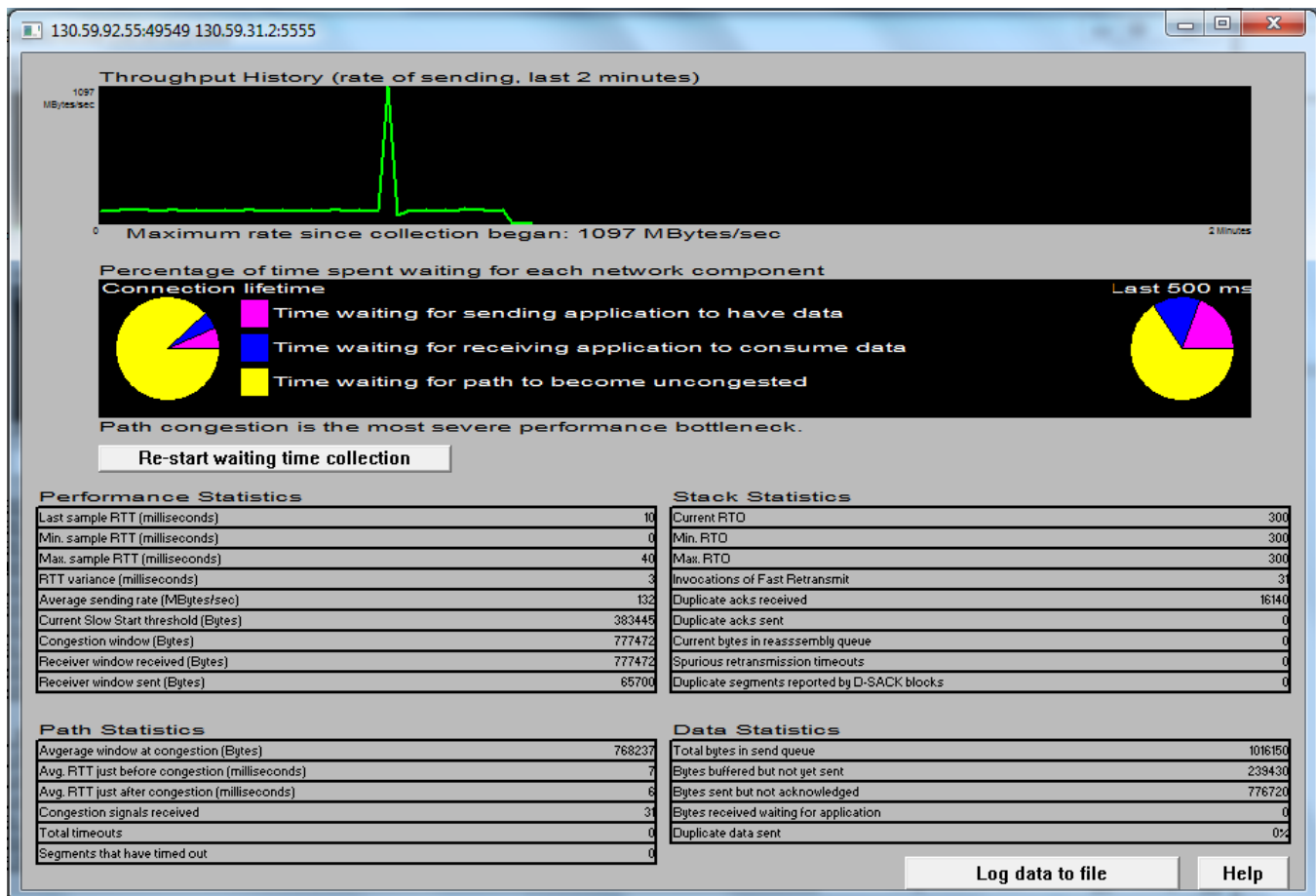
Screenshots:

- TCP Analyzer Connection selection:

Local host	Local port	Remote host	Remote port	Owning PID	State
momp2	445	momp2	0	4	LISTEN
momp2	2869	momp2	0	4	LISTEN
momp2	8093	momp2	0	1792	LISTEN
momp2	49152	momp2	0	500	LISTEN
momp2	49154	momp2	0	468	LISTEN
momp2	49156	momp2	0	580	LISTEN
momp2	49225	momp2	49226	3676	ESTABLISHED
momp2	49227	momp2	49228	3676	ESTABLISHED
momp2	49228	momp2	49227	3676	ESTABLISHED
momp2	49226	momp2	49225	3676	ESTABLISHED
momp2	445	momp2	0	4	LISTEN
momp2	2869	momp2	0	4	LISTEN
momp2	10243	momp2	0	4	LISTEN
momp2	49153	momp2	0	996	LISTEN
momp2	139	momp2	0	4	LISTEN
momp2	49155	momp2	0	556	LISTEN
momp2	49156	momp2	0	580	LISTEN
momp2	49154	momp2	0	468	LISTEN
momp2	49152	momp2	0	500	LISTEN
momp2	5357	momp2	0	4	LISTEN
momp2	554	momp2	0	2924	LISTEN
momp2	135	momp2	0	800	LISTEN
momp2	3826	momp2	0	440	LISTEN
momp2	49155	momp2	0	556	LISTEN
momp2	49153	momp2	0	996	LISTEN
momp2	10243	momp2	0	4	LISTEN
momp2	5357	momp2	0	4	LISTEN
momp2	554	momp2	0	2924	LISTEN
momp2	135	momp2	0	800	LISTEN
momp2.mpp.switch.ch	139	momp2	0	4	LISTEN

Help Show IP addresses Load a log file Enable EStats Collection

TCP Connections Display

- TCP Analyzer Example connection with congested path:

130.59.92.55:49508 130.59.31.2:5555

Throughput History (rate of sending, last 2 minutes)

18446744072 GBytes/sec

0   Maximum rate since collection began: 18446744072 GBytes/sec   2 Minutes

Percentage of time spent waiting for each network component

Connection lifetime

Last 500 ms

■ (magenta) Time waiting for sending application to have data

■ (blue) Time waiting for receiving application to consume data

■ (yellow) Time waiting for path to become uncongested

Path congestion is the most severe performance bottleneck.

Re-start waiting time collection

Performance Statistics

Last sample RTT (milliseconds)	0
Min. sample RTT (milliseconds)	0
Max. sample RTT (milliseconds)	40
RTT variance (milliseconds)	3
Average sending rate (KBytes/sec)	80466
Current Slow Start threshold (Bytes)	374417
Congestion window (Bytes)	653187
Receiver window received (Bytes)	777472
Receiver window sent (Bytes)	65700

Stack Statistics

Current RTO	300
Min. RTO	300
Max. RTO	300
Invocations of Fast Retransmit	25
Duplicate acks received	13007
Duplicate acks sent	0
Current bytes in reasssembly queue	0
Spurious retransmission timeouts	0
Duplicate segments reported by D-SACK blocks	0

Path Statistics

Avgerage window at congestion (Bytes)	767687
Avg. RTT just before congestion (milliseconds)	8
Avg. RTT just after congestion (milliseconds)	6
Congestion signals received	25
Total timeouts	0
Segments that have timed out	0

Data Statistics

Total bytes in send queue	253952
Bytes buffered but not yet sent	0
Bytes sent but not acknowledged	253952
Bytes received waiting for application	0
Duplicate data sent	0%

Log data to file   Help

- TCP Analyzer Connection with small buffers:

130.59.92.55:49549 130.59.31.2:5555

Throughput History (rate of sending, last 2 minutes)

1097 MBytes/sec

0

Maximum rate since collection began: 1097 MBytes/sec

2 Minutes

Percentage of time spent waiting for each network component

Connection lifetime

Last 500 ms

■ Time waiting for sending application to have data

■ Time waiting for receiving application to consume data

■ Time waiting for path to become uncongested

Path congestion is the most severe performance bottleneck.

Re-start waiting time collection

Performance Statistics

Last sample RTT (milliseconds)	10
Min. sample RTT (milliseconds)	0
Max. sample RTT (milliseconds)	40
RTT variance (milliseconds)	3
Average sending rate (MBytes/sec)	132
Current Slow Start threshold (Bytes)	383445
Congestion window (Bytes)	777472
Receiver window received (Bytes)	777472
Receiver window sent (Bytes)	65700

Stack Statistics

Current RTO	300
Min. RTO	300
Max. RTO	300
Invocations of Fast Retransmit	31
Duplicate acks received	16140
Duplicate acks sent	0
Current bytes in reasssembly queue	0
Spurious retransmission timeouts	0
Duplicate segments reported by D-SACK blocks	0

Path Statistics

Avgerage window at congestion (Bytes)	768237
Avg. RTT just before congestion (milliseconds)	7
Avg. RTT just after congestion (milliseconds)	6
Congestion signals received	31
Total timeouts	0
Segments that have timed out	0

Data Statistics

Total bytes in send queue	1016150
Bytes buffered but not yet sent	239430
Bytes sent but not acknowledged	776720
Bytes received waiting for application	0
Duplicate data sent	0%

Log data to file   Help

– Main.ChrisWelti - 12 Jan 2010