Data sheet

ZEN
IP MONITOR

Death, Taxes & Response Times

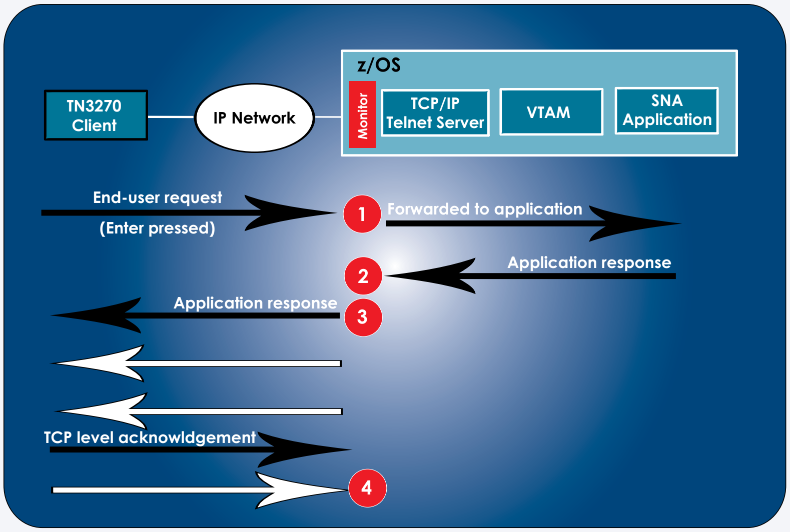
Like death and taxes, another of life's certainties is that, at some point, users will complain about Response Times. Forget about I/O rates, packet counts, connection details or any one of a hundred other ways of measuring network performance - these mean nothing to the user. The one thing they can relate to is the amount of time it takes to get a response to an enquiry once the enter key has been depressed. They simply measure system performance by what they perceive to be Response Time.

Measuring Response Time

For some protocols, such as TN3270 and TN3270E, the measurement of response time is relatively simple. Since the TN3270 protocols enforce a single request/response structure, the start and end of a transaction is easy to identify and, therefore, measure (see Fig.1).

For other protocols the measurement of response time is not so straightforward. Full duplex peer-to-peer protocols, where either end of a connection can send data at any time, do not usually request a response. Consequently, it is not possible to demonstrate response time. A more practical measure is to look at Network Transit Time (see figure 3).

Figure 1: Typical T3270 Transaction Response Time



Application Response Time = Timestamp **2** minus Timestamp **1**
Network Delay = Timestamp **4** minus Timestamp **3**
Total Response Time = Timestamp **4** minus Timestamp **1**

Monitoring TN3270 Response Time

Many products claim to monitor TN3270 response time while they actually do nothing more than issue a PING command to an IP address and offer the Round Trip Time as Response Time. This is not valid for a number of reasons:

- TN3270 is TCP based whereas PING is ICMP based. Each protocol is handled differently in routers and many firewalls are actually configured to exclude ICMP traffic. As a result, it is possible that the packets from the PING will travel a different route to those from TN3270, thereby making the Round Trip Time different from the actual response Time.
- A PING is usually 32 bytes while TN3270 session data can be anything up to 2K. Furthermore, its size will vary during the course of a session. Since the PING is usually small and of a fixed size, it will not be affected by fragmentation, window size and retransmissions that can, and will, affect TN3270 response times if they are occurring in your system.
- A PING does not contain user data. As a result, it cannot truly represent the Response Times that users are experiencing.

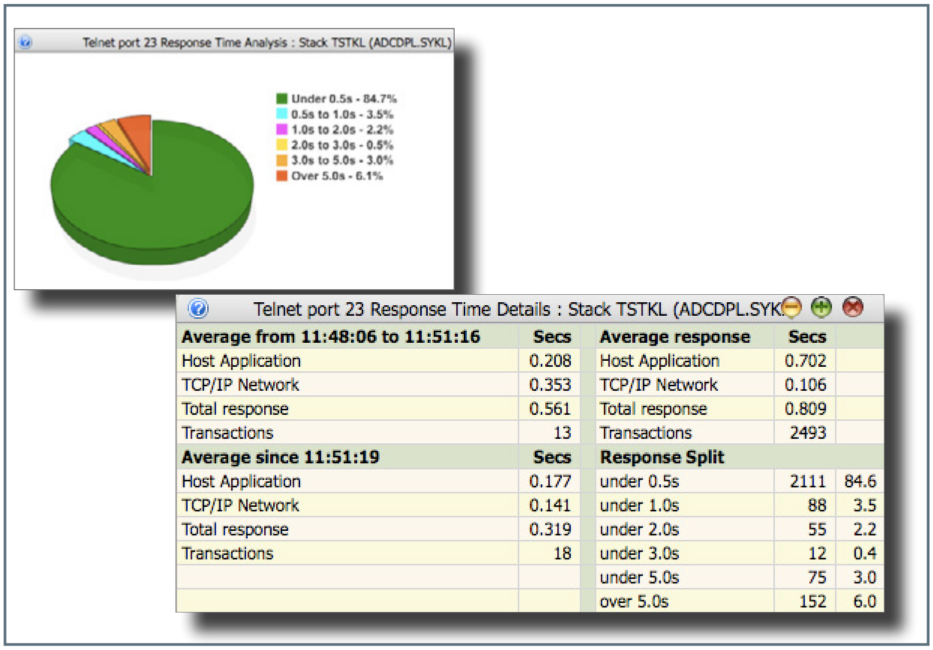
WILLIAM
DATA SYSTEMS

ZEN IP MONITOR (ZIM), formerly known as IMPLEX, is able to monitor true TN3270 Response Times. It has been developed in line with RFC2562 which defines the methodology for performing response time data collection for TN3270E servers. Although IMPLEX is not a TN3270E server, it has applied the same technique and extended the methodology to measure response time for TN3270 as well as TN3270E. Since Implex sees every packet that traverses the IP stack, it is able to record the time of every request and its associated response (see Fig.2).

Response Time can be measured at the Port, Connection and External Host level. These can all be viewed in real-time and alert monitoring can be activated, sending alerts to SNMP, NetView, the console or by e-mail.

In this way, users of ZIM can be confident of the level of service given to the TN3270 users.

Figure 2: ZEN IP MONITOR - IMPLEX Detailed Response Time Statics Displays for TN3270



Telnet port 23 Response Time Details : Stack TSTKL (ADCDPL.SYKL

Average from 11:48:06 to 11:51:16	Secs	Average response	Secs	
Host Application	0.208	Host Application	0.702	
TCP/IP Network	0.353	TCP/IP Network	0.106	
Total response	0.561	Total response	0.809	
Transactions	13	Transactions	2493	
Average since 11:51:19	**Secs**	**Response Split**		
Host Application	0.177	under 0.5s	2111	84.6
TCP/IP Network	0.141	under 1.0s	88	3.5
Total response	0.319	under 2.0s	55	2.2
Transactions	18	under 3.0s	12	0.4
		under 5.0s	75	3.0
		over 5.0s	152	6.0

Monitoring Other Applications

For services such as DB2, CICS or Websphere, the concept of response time only exists if the end application enforces the single request/single response structure as in TN3270. Since IMPLEX has no specific knowledge of the application logic and does not, therefore, present response times in the same way as it would for TN3270 traffic, it offers Network Transit Time as an alternative to aid users in measuring the performance of these applications (see Fig.3).

The Network Transit Time component can be activated for specific ports (e.g. the CICS and DB2 ports) and used to measure the network throughput to the end user from these applications. The throughput data can be presented at the application, remote host, or connection level in terms of the transit time, in milliseconds, for the message to be transmitted across the network. Data is for different message sizes so the system engineer can see how message size affects transmission times.

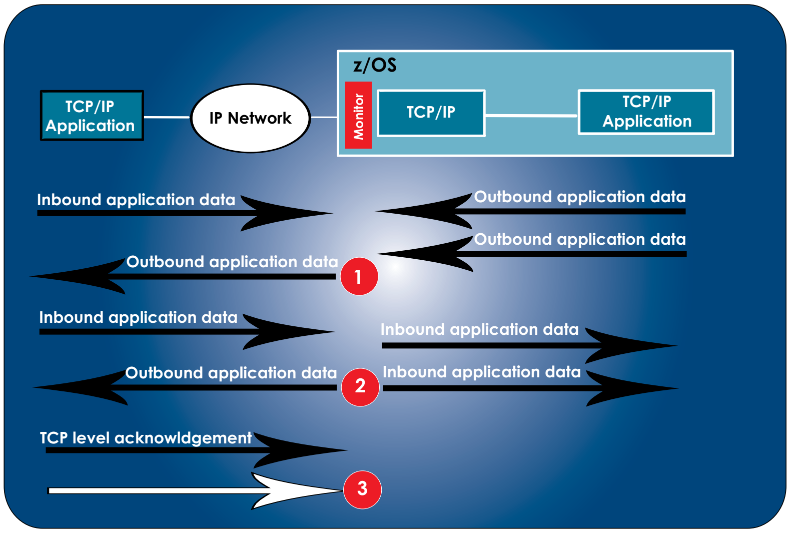


Figure 3: Typical Full-Duplex (TCP/IP) Data Flow Showing Network Transit Time

Figure 3: Remote TCP/IP application sends data at the same time and on the same connection as the local TCP/IP application.

1 The monitoring tool takes a timestamp and records data length
2 Length of additional data is recorded and time-stamped
3 Network Transit Time is calculated when TCP confirms all bytes have been acknowledged

Monitoring FTP

There is no response time associated with FTP. Because of the structure of the protocol, the only meaningful measurements of activity are either:

- Total time to transfer a file
- Data throughput rate

Measuring transfer time is of limited use because it will obviously vary depending on the file size.

A more practical measurement for FTP is the rate of data throughput, such as KBytes per second.

ZIM can monitor and report on all FTP transmissions and highlight the average throughput time for all FTP activity or for a specific remote host. As with other services, ZIM is able to issue alerts based on both high and low levels of activity. For comprehensive ftp security and management use ZEN FTP CONTROL (ZFC), formerly known as FTPALERT.

ZEN IP MONITOR Answers The Response Time Problem

With ZIM, users are able to view the true response times given to their users and not simply some crude approximation - a PING, after all, is just a PING and not a true reflection of user experience.

Having accurate information about achieved service levels and being able to demonstrate how specific areas of network performance relate to response time problems puts the network technician in powerful position when defending performance issues.

ZEN IP MONITOR

Optimize Network Performance

Pinpoint Issues Before They Become a Problem

ZEN

William Data Systems (WDS) is a pioneer of specialized z/OS network management solutions. Established in 1993, we are an independent global organization that provides innovative solutions to run mainframe networks efficiently and securely. ZEN, the WDS network management suite, offers a selection of user-friendly and cost-effective solutions to meet your unique needs. To overcome both business and technology challenges, WDS provides customers with licensing and pricing terms that are as flexible as our solutions.

WDS supports customers worldwide in sectors such as finance, banking and manufacturing, and our client list includes Fortune 100 companies and government agencies. WDS is an IBM Business Partner and a member of the IBM PartnerWorld for Developers program. We are committed to the global z/OS networking market and to leading the way with innovative solutions through the latest advances.

Business Partner IBM
Authorized
System z

To learn more about
WDS ZEN solutions,
for support or to contact
our offices, visit
www.willdata.com

WILLIAM
DATA SYSTEMS