Lost without a trace?

Simon Cooper looks at what users might like to see in a network trace – and takes a look at how those features are realized in one such product.

A trace can be a really useful way of debugging problems with networks or applications. In fact sometimes it's the only way. The kind of low-level information found in a trace often provides a unique clue as to the root cause of a problem. Despite this, many mainframe professionals use tracing solely as a last resort, when all other attempts to resolve a problem have failed. This is due to the perceived difficulty of taking a trace, as well as the complexities of interpreting the resulting output.

Traces can contain vast amounts of data, all of which may potentially be required, but the volume of data can obscure the very problem you're trying to identify. Interpreting the trace can be equally problematic, requiring knowledge of IPCS to browse and analyze CTRACE or GTF datasets, as well as a familiarity with many IBM manuals, an understanding of trace record layouts, TCP/IP control codes, the format and meanings of VTAM sense bytes, 3270 order codes and so on, just to begin to interpret a trace. Consequently, the job of finding a problem using a trace is usually a long, labour-intensive, and tedious task. Under these circumstances it's not surprising that trace taking is often the last resort of an exasperated technician.

Keeping it simple

The introduction in 1994 of EXIGENCE from William Data Systems brought an uncomplicated and straightforward approach to tracing network-related connectivity, response time or performance problems. Now known as ZEN TRACE & SOLVE (ZTS), the product makes it simple to not only take a trace but, perhaps more importantly, interpret the trace data, guiding the user to the problem area and usually suggesting a solution within minutes. By eliminating all the difficulties associated with trace capture and analysis, organizations can save countless hours and thousands of dollars.

Defining and capturing traces

ZTS enables you to easily define and initiate a variety of trace types, including TCP/IP, VTAM, and even NCP line traces, through one of three user interfaces (UI) – Web browser, 3270, and PC client (see Figure 1). Trace definitions are all done from within the UI, requiring no batch jobs to be started and therefore no knowledge of JCL is required.

For TCP/IP traces, you define only a description and the name of the address space running TCP/IP (and optional filters) for trace capture. Traces can be captured in up to seven address spaces simultaneously, tracing all IP packet exchanges. Enhanced facilities are available for several popular applications, for example TCP, UDP, ICMP, FTP, LPR, RIP, NCPROUT, OSPF, GRE, and Enterprise Extender protocols.

For VTAM traces, the only piece of information you need to provide is a brief description of the trace and the LU name (the terminal or application) that is causing the problem. VTAM traces will capture all exchanges between LUs, LU 6.1, LU 6.2, LU types 0, 1, 2, 3 and so on.

Tracing intermittent problems

Of course it's not always possible to know in advance when a problem might occur, which may mean you need to leave a trace running for a long period, potentially creating an enormous trace. ZTS has a neat solution to this, allowing you to define a 'Wrap Mode' trace, which only uses a finite amount of space for trace recording, looping around and re-sequencing the trace entries into chronological order once the trace is stopped.

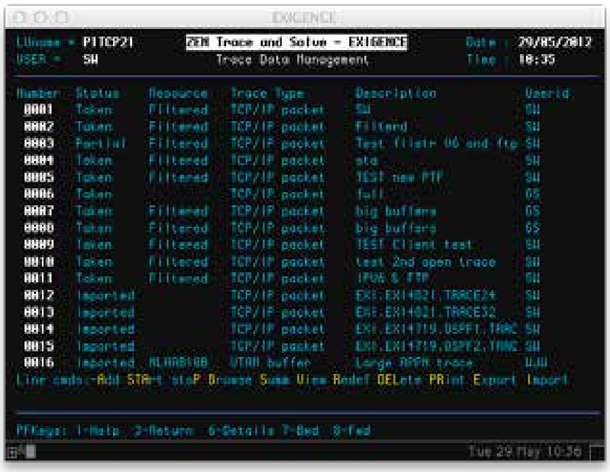
Automatically taking and merging multiple traces

Tracing in a complex multi-LPAR and/or multi-processor environment would normally involve the taking and examination of multiple traces. For example, you may need to trace a single client IP address that has many connections to several systems. The difficulty is compounded if an IP client connects to a service running on multiple systems using dynamic VIPA, because it is impossible to be sure with which system the connection will be made.

In such environments, usually the only option available for problem diagnosis is to initiate traces on each individual system. This is difficult enough. Once taken, all the individual trace records need to be sorted into chronological order before being interpreted to try and diagnose the cause of the problem. Assuming the technician has the knowledge and experience to carry out this task, it is still a time consuming, and therefore costly process.

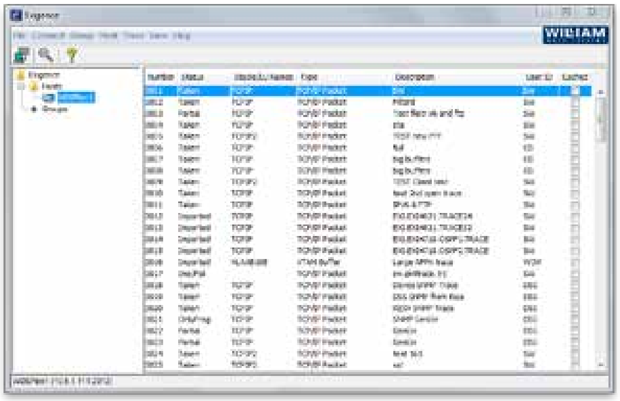
The ZTS solution is to allow the definition and capture of multiple IP traces at once. Known as “Group Trace”, it’s basically the same as a ‘normal’ trace except that it can be simultaneously started on a group of systems with the resulting trace output viewed as if it had been taken on a single system, with the trace entries interleaved according to their capture time.

New to Version 5 of ZTS, you can now synchronize group trace entries by normal, relative or incremental time, giving you a huge advantage when analysing trace data spanning multiple systems in different time zones. You can also now define Group traces on-the-fly; it is no longer necessary to pre-define the hosts on which a group trace is to be captured. You can even build a group trace from a set of traces that were not originally captured as part of a group trace (eg imported traces).

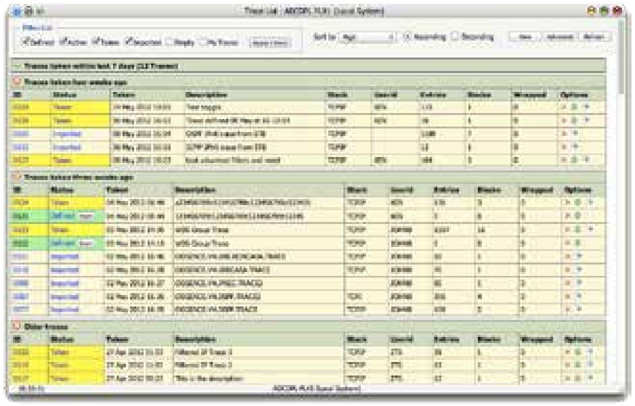


```
LUname = PITCP21          ZEN Trace and Solve - EXIGENCE       Date : 29/05/2012
USER =   SW                  Trace Data Management             Time : 10:35

Number  Status    Resource   Trace Type     Description                 Userid
 0001   Taken     Filtered   TCP/IP packet  SW                          SW
 0002   Taken     Filtered   TCP/IP packet  Filterd                     SW
 0003   Partial   Filtered   TCP/IP packet  Test filetr 06 and ftp      SW
 0004   Taken     Filtered   TCP/IP packet  sta                         SW
 0005   Taken     Filtered   TCP/IP packet  TEST new PTF                SW
 0006   Taken                TCP/IP packet  full                        GS
 0007   Taken     Filtered   TCP/IP packet  big buffers                 GS
 0008   Taken     Filtered   TCP/IP packet  big buffers                 GS
 0009   Taken     Filtered   TCP/IP packet  TEST Client test            SW
 0010   Taken     Filtered   TCP/IP packet  test 2nd open trace         SW
 0011   Taken     Filtered   TCP/IP packet  IPV6 & FTP                  SW
 0012   Imported             TCP/IP packet  EXI.EX14021.TRACE24         SW
 0013   Imported             TCP/IP packet  EXI.EX14021.TRACE32         SW
 0014   Imported             TCP/IP packet  EXI.EX14719.OSPF1.TRAC      SW
 0015   Imported             TCP/IP packet  EXI.EX14719.OSPF2.TRAC      SW
 0016   Imported  NLHAB10B   VTAM buffer    Large APPN trace            WJW
Line cmds:-Add STArt stoP Browse Summ View Redef DELete PRint Export Import

PFKeys: 1-Help  3-Return  6-Details  7-Bwd  8-Fwd
                                                          Tue 29 May 10:36
```

Original 3270 interface circa 1994



PC java^{TM} client circa 2005



ZEN TRACE & SOLVE - 2013

Figure 1: The evolving EXIGENCE UI

Analysing a captured trace

Having captured a trace, it can then be viewed in a number of different formats, from a summarized view of the session exchanges between socket pairs or LUs known as the Flow display, to an expanded format that shows data structure breakdowns right to the individual bit level, with settings with descriptions provided.

Any 3270 data streams in a trace can be displayed in their entirety either in hex or with all of the control orders interpreted, even when the data stream is encapsulated as in the case of Enterprise Extender. This is particularly useful when an error has been caused by a fault in transmitted data. You can switch between the different display formats with no loss of context.

ZTS analyses the trace data, automatically scanning and highlighting any negative or exception responses and pairing them with the original request. ZTS can even explain what the highlighted problem areas mean. ZTS not only provides an explanation of the data in error, but also pinpoints the most likely cause of the problem and in some cases can even suggest a solution.

ZTS also provides comprehensive search functions, enabling you to scan a trace, either forwards or backwards, for any TCP/IP or VTAM condition, data sequence, or even down to a single bit in a specific byte. This is particularly useful when you already have a good idea of what a problem might be and just want your suspicions confirmed.

Built-in knowledge base

ZTS includes a comprehensive ‘Explain’ function. This enables anyone, from Help Desk staff to trace experts to find information on any TCP/IP or VTAM/3270 term, sense code, 3270 order code, and so on. Searching through many IBM manuals to find the meaning of a particular bit setting becomes a thing of the past with ZTS.

ZTS features at a glance

- Enables online trace management – no batch set-up required
- Supports simultaneous capture of multiple
- IP and SNA traces
- Formats and translates all trace data prior to display
- Displays all data flows with meaningful annotation
- Enables display mode switching without loss of context
- Supports powerful filtering techniques enabling traces to be targeted at:
  - Defined Applications: (Telnet, FTP, EE etc)
  - Defined Protocols: UDP, ICMP, TCP, SASP and specific numbered protocols
  - Defined Port numbers
  - Defined IP addresses
  - LU to LU sessions
  - LU to Application (eg CICS sessions)
- Allows individual trace file sizes to be minimized via the ‘Wrap Mode’ feature
- ‘Peek’ feature allows traces to be browsed “in flight”
- Simplifies import and evaluation of externally captured traces
- Simplifies export, in IBM-recognizable or libpcap format, of captured traces
- Manages all trace types including:
  - IP Packet and Data Traces
  - EE Traces
  - VTAM buffer and I/O Traces
  - VTAM Extended Trace (XTD)
  - VTAM Internal Trace (VIT)
  - NCP 3745 Trace including Scanner, Generalized PIU and TG Traces
  - 3746/900 /950 Trace Import
- Enhanced analysis facilities for TCP, UDP, ICMP, FTP, LPR, RIP, NCPROUT, OSPF, GRE and EE protocols
- Incorporates a 3270 and ZEN browser UI. PC client also available
- Provides comprehensive help on any IP, VTAM and/or 3270 terminology, message or sense code
- Full support for IP Version 6
- Supports trace printing
- Full audit of trace activities.

Special support for Enterprise Extender

WDS have long been advocates of Enterprise Extender (EE), recognizing its importance as a means of preserving investment in SNA while allowing the exploitation of the latest advances in IP networking technologies. We have developed a number of unique products and features that address shortcomings with the management of EE, including specialist products for monitoring, encrypting, and authenticating EE data streams.

Tracing in an EE environment presents unique challenges, because although the protocol carrying the data is IP-based, the payload data itself is SNA in origin. The Enterprise Extender support in ZTS enables you to expand all the EE headers, stripping away IP-related material to provide an unencumbered view of the underlying SNA (TH, RH, and RU) payload.

A new user-interface for EXIGENCE

ZTS continues to be at the forefront of network problem determination and is a central component of our ZEN network management suite. The latest version of ZEN TRACE & SOLVE (Version 5), is a no-cost upgrade for customers and brings the proven advantages of our flexible and powerful ZEN User Interface to all EXIGENCE customers.

Innovative Web view

As a major component of the ZEN suite of Network Management solutions, the ZTS browser interface benefits from the innovative design provided by ZEN. No special desktop software is required and, unlike other browser-based solutions, it has the distinct advantage of not requiring a separate Web server.

A Web server is usually part of a three-tier system comprising a network data collector on the z/OS host, a separate Web server where the Web pages are generated, and a client for data display. A three-tier approach has many drawbacks. It adds cost (additional hardware, software, and configuration), adds complexity to the set-up and maintenance of the monitor system, adds overhead (additional bandwidth load from the extra connections), and provides an additional point of failure.

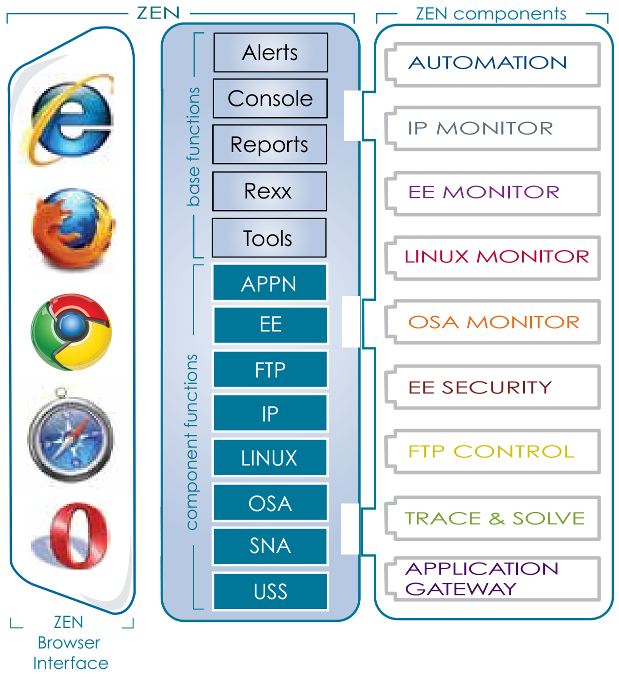


Figure 2: ZEN's two-tier architecture

The ZTS user interface is part of a two-tier architecture (see Figure 2) that takes advantage of the core strengths of ZEN – namely, efficient, high-speed, and low-overhead data delivery. Proving that less really is more, this innovative two-tier approach has a number of benefits over three-tier systems as it:

- Reduces costs without the need for additional hardware or software
- Simplifies implementation since client software is not required
- Deploys rapidly, providing immediate access to trace data from a standard web browser
- Necessitates little or no processor overhead because all graphical formatting is performed inside the browser
- Provides single interface for all your network management needs

- Is SMP/E maintainable, enabling rapid application of new features and services.

Importing and exporting traces

ZTS doesn't just work with traces taken within the product. It also allows traces to be imported from:

- IBM's IP packet traces
- IBM's VTAM Buffer traces
- OSAENTA traces
- libpcap traces (eg Wireshark, Sniffer).

Once a trace has been imported, you have the full power of all the ZTS commands and Expansion functions to help you analyse it.

You may also export ZTS traces to a disk dataset so that they can be sent elsewhere for further analysis. IP traces are exported in CTRACE format, SNA traces in GTF format, and OSAENTA and libpcap traces in their respective formats.

Automatic event tracing

The ZTS command interface can be used to Add, Redefine, Start and Stop traces allowing event-based dynamic trace management activities to be performed, for example, to define and start a trace automatically dependent upon some other event in the system.

A tool of first resort

The traditionally complex task of tracing has usually been undertaken by a diminishing number of old-school skilled technicians. However, the availability of modern technologies improves accessibility to this extremely useful problem-solving technique for the next generation of technicians, removing complexity and turning tracing into a tool of first resort. ■

Simon Cooper has worked in the Independent Software Vendor market for nearly twenty-five years and has held a variety of technical, sales, and marketing roles in addition to his current position as head of business development at WDS.

William Data Systems (WDS) is a pioneer of specialized IBM System z network management solutions. Established in 1993, we are an independent global company 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 help customers 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 across all vertical markets 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.