MAINFRAME TCP/IP MANAGEMENT

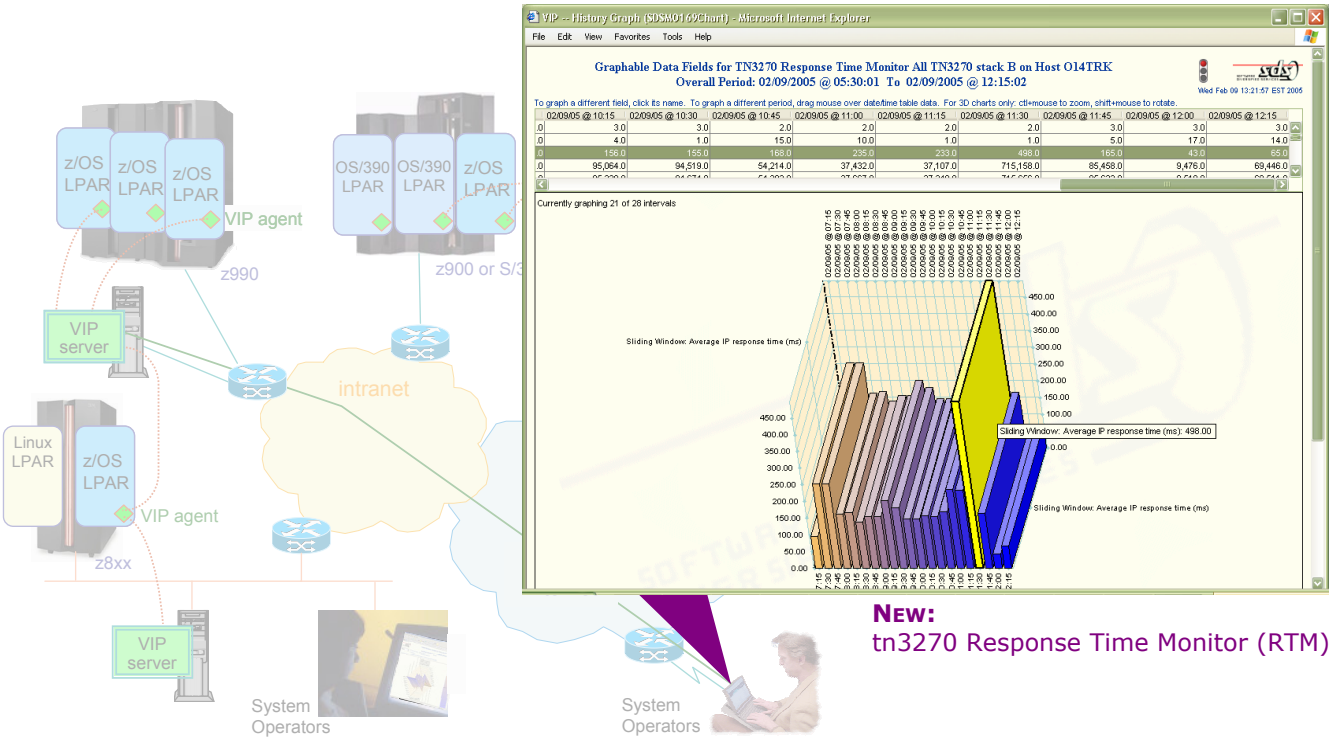
FOR ZERO DOWNTIME, HIGH PERFORMANCE OPERATIONS

SOFTWARE DIVERSIFIED SERVICES (SDS)

VITAL SIGNS VISIONNET IP MONITOR (VIP) v4

Mastering Complexity
& Monitoring Response

A WHITE PAPER

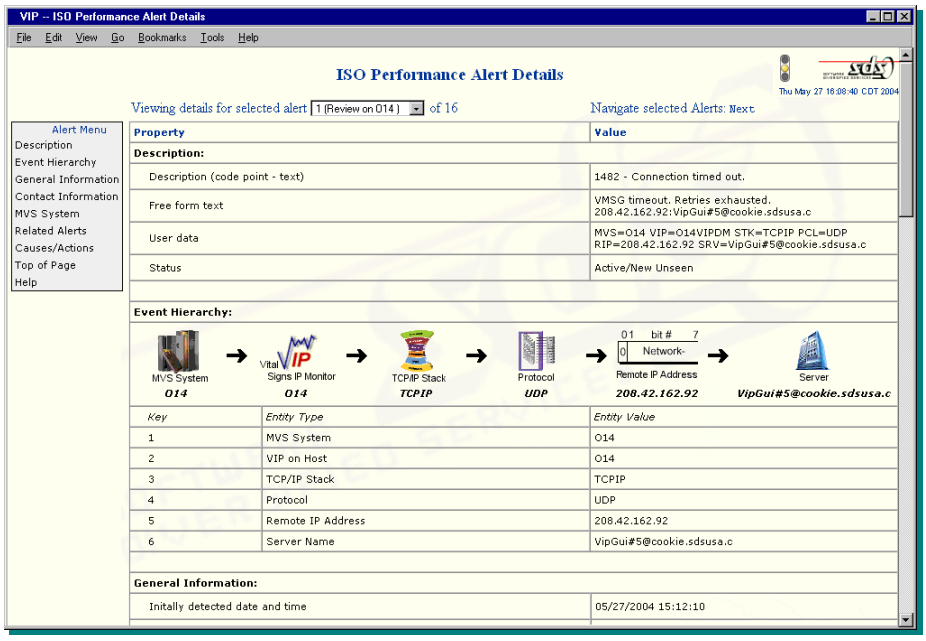


NEW:
tn3270 Response Time Monitor (RTM)

Developed for SDS:
by Anura Gurugé
February 2005

SOFTWARE DIVERSIFIED SERVICES
www.sdsusa.com

TABLE OF CONTENTS



Performance alert details

Mainframe TCP/IP Management

for Zero Downtime, High Performance Operations

Software Diversified Services (SDS)

Vital Signs VisionNet IP Monitor (VIP) v4

Mastering Complexity
& Monitoring Response

TCP/IP has now firmly displaced SNA as the preferred and strategic means for mainframe networking. That is beyond refute. SNA mission critical applications, these days, are successfully sustained across TCP/IP networks through a combination of Enterprise Extender (EE), tn3270(E) and Web-to-host. Thus to realize *'zero downtime'* mainframe operations, with crisp and consistent response times for interactive users, one has no choice but to master TCP/IP management and response time monitoring (RTM).

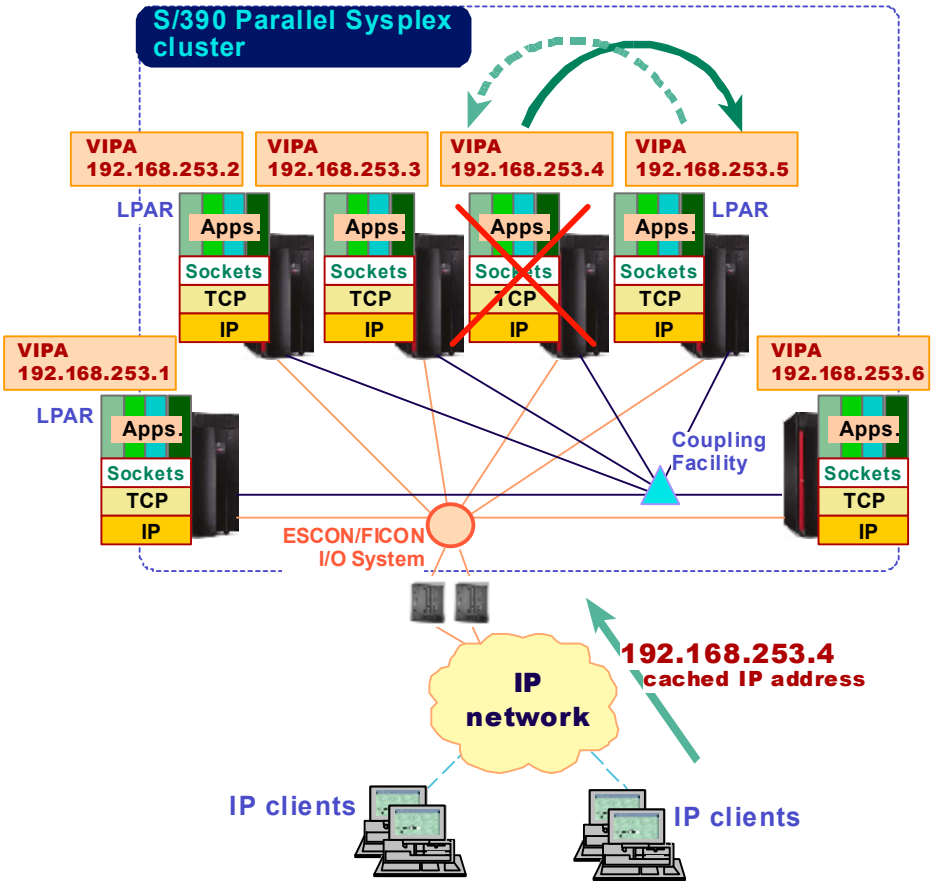
Mainframe TCP/IP networking is invariably complex, often challenging, and sometimes a bit confounding. This is to be expected given what can be involved and what is at stake.

Mainframe TCP/IP networking can involve multiple stacks per LPAR, virtual addresses, gigabit OSA interfaces, HiperSockets, dynamic VIPA takeovers across a sysplex, disparate application protocols, many hosts, and lots of connectionless interactions. There is also a need to be cognizant of routers, switches, firewalls, and possibly even Linux LPARs – with performance, in particular '3270' response times, always a concern, and security a nagging worry.

To stay on top of all of this, to deliver *'zero downtime'* operations, you need a good mainframe network monitor that is probing, incisive, thorough and nimble – that, moreover, works in true real-time. Otherwise *"you will be flying blind"*. Having a comprehensive RTM capability is an added bonus – *like having radar*. It permits you to see potential problems way out and take evasive action before they cause any disruptions.

A good mainframe network monitor also needs to be simple, intuitive and easy-to-use. Otherwise it will hinder rather than help. In regards to this, the incomparable Leonardo da Vinci said it best:

"Simplicity is the ultimate sophistication"



TODAY'S MAINFRAME TCP/IP NETWORKING CAN BE COMPLEX IN THAT IT CAN INVOLVE MULTIPLE HOSTS, MANY LPARS, VIRTUAL IP ADDRESSES AND EVEN FEATURES SUCH AS DYNAMIC VIPA TAKEOVER IN THE EVENT OF AN LPAR FAILURE.

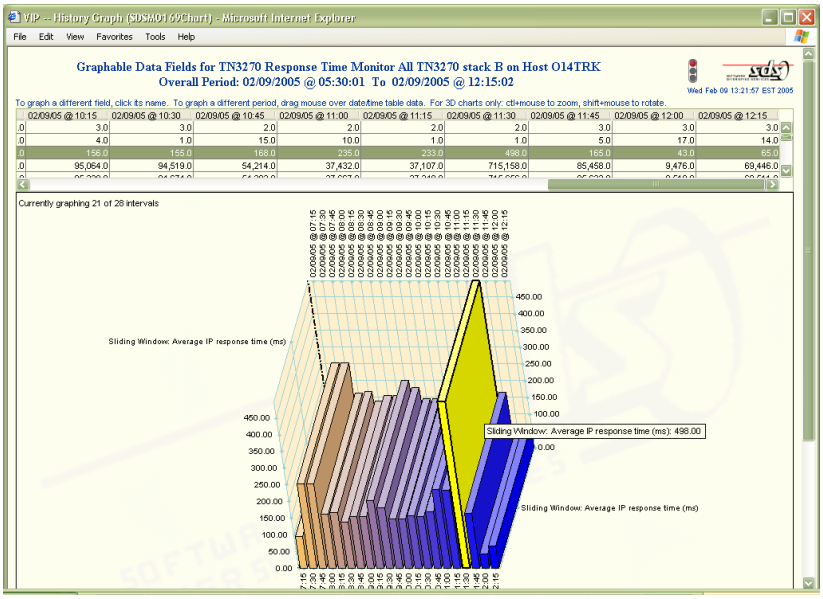
Mainframe TCP/IP networking, though now stable, robust and capable of sustaining mission-critical applications, is, nonetheless, very different, in many basic ways, from SNA. SNA, per contemporary vernacular, was highly controlling. The mainframe-resident SSCP had its tentacles into everything, all the time, and tried to keep tabs on what everybody was up to.

Not so with IP networking. IP is ultra laid-back and eschews control sessions. It permits connectionless interactions and does not worry about data packets that never reach their destination. This is a very different networking paradigm to what today's mainframe professionals are used to. A good mainframe TCP/IP network monitor thus needs to help mainframe professionals to smoothly bridge this divide and enable them to maintain optimum system/network performance despite the paradigm shift. Providing all the pertinent management data, including detailed response time statistics for the interactive 3270 sessions, in easy to follow graphical form is a key step in fulfilling this objective. Automated, 'intelligent' alarms, when certain thresholds are crossed, are also imperative.

A good mainframe TCP/IP network monitor should let system operators focus all of their attention on monitoring and managing the network without having to contend with obfuscating processes and hard to fathom data displays. They should have total confidence in the proven power and capabilities of their TCP/IP monitor and know that their monitor will automatically notify them of potential problems – ideally well before they become 'show-stoppers'.

Continuous, intelligent response time monitoring, with multiple preset threshold alerts is invariably a very accurate measure of overall system/network health and stability. Sudden, unexpected changes in response time characteristics tend to be a leading-edge indicator that something has changed within the overall system. Degradation in response times, in mission-critical mainframe networks, can also results in lost opportunity costs [e.g. inability complete financial trades prior to changes in price], decrease in user productivity, and a flurry of calls to the help desk by disgruntled users. A comprehensive RTM scheme that quickly detects changes in response times and automatically raises appropriate alerts thus serves as an invaluable 'early warning' mechanism of potential system, network or application problems.

With these basic parameters nailed down, one can go on to categorize the essential characteristics of a good mainframe TCP/IP network monitor. These characteristics are listed in the table on page 6. However, to make these categorizations even more pragmatic and useful, they have been further divided into *"must-have"* imperative features, and *"icing on the cake"* highly-desirable attributes. The monitor that you choose should include, without any caveats, all the features listed in the "must have" column, and ideally most of those listed in the other column.



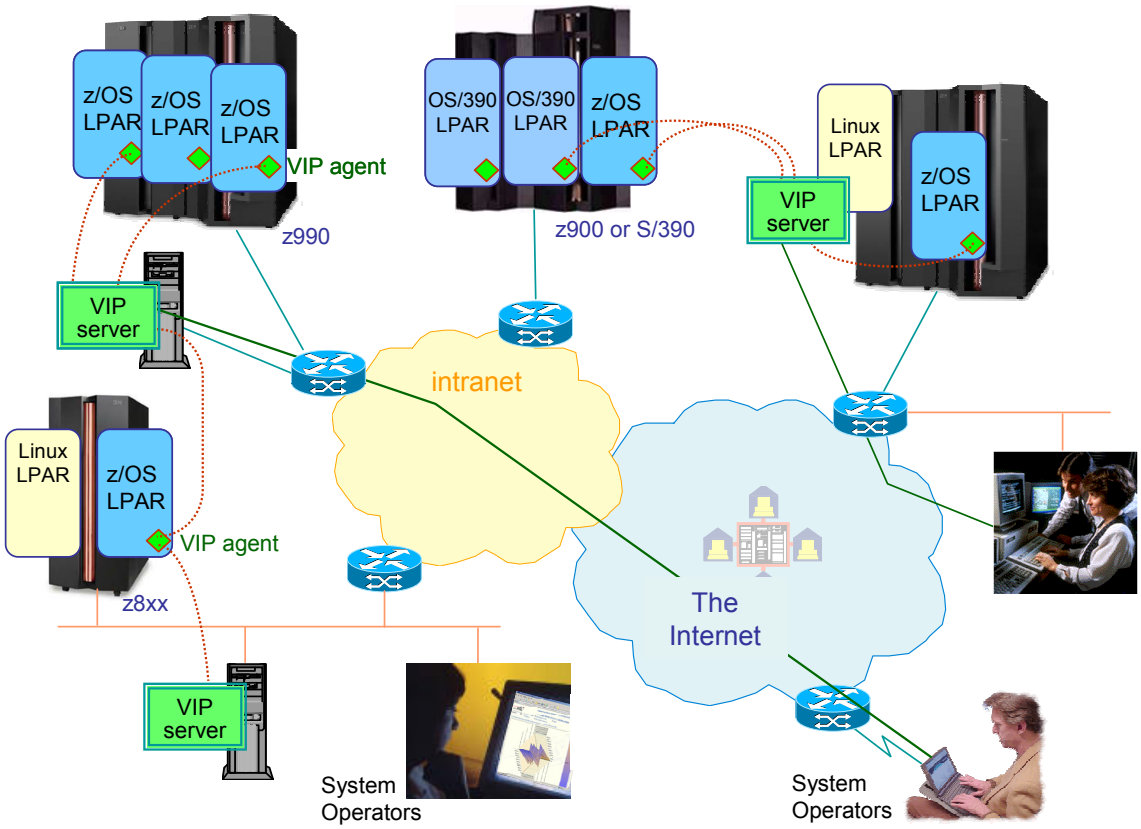
THE NEW TN3270 RTM IN VIP V4 GRAPHICALLY DEPICTING A SLIDING WINDOW AVERAGE OF RESPONSE TIMES OVER A 2 HOUR PERIOD – WITH A 'HOT-SPOT' CAPABILITY ON EACH 'BAR' ON THE GRAPH THAT IMMEDIATELY EXPANDS THAT COLUMN TO PROVIDE THE EXACT STATISTICS ASSOCIATED WITH IT.

CHARACTERISTICS OF A GOOD MAINFRAME TCP/IP NETWORK MONITOR	
IMPERATIVE	**HIGHLY-DESIRABLE**
➢ ability to monitor multiple LPARs per mainframe and multiple mainframes from a single screen. ➢ accurate, *"up to the second"* at-a-glance status maps of the entire network. ➢ instantaneous, at-a-glance visibility of all alerts. ➢ obtain the necessary network management statistics, data and performance numbers directly from a TCP/IP stack. ➢ incisive response time monitor (RTM), compliant with the RFC 2562 standard, for IBM's tn3270(E) server. ➢ immediate access to both current and historic FTP and telnet activity reports. ➢ remote host monitoring to have visibility of external systems, such as routers, switches and firewalls. ➢ being nimble, light and low-overhead so that it is responsive – and furthermore does not get in the way of production workloads. ➢ comprehensive support for all OSA and OSA-Express interfaces. ➢ intelligent monitoring of tn3270(E) with SNA correlation; e.g. LU names, unused LUs etc. ➢ PING and traceroute capabilities. ➢ NetView interoperability.	➢ direct retrieval of management data from the TCP/IP stacks, augmented, where necessary, with full SNMP access and packet tracing. ➢ browser-based, highly-visual, point-and-click monitoring and management complemented by a command line interface. ➢ support for Enterprise Extender (EE) so that all connection details are always available. ➢ fast, auto-discovery of all stacks, applications and interfaces. ➢ agent/server based architecture to minimize mainframe overhead while affording maximum deployment flexibility. ➢ integrated DNS look-up. ➢ application-specific round-trip time measurements. ➢ access to summarized OSA performance data reports on physical channel, LPAR utilization, and OSA usage. ➢ ability to capture RTM on multiple criteria (with overlap, if necessary); e.g. at a subnet as well as individual session basis. ➢ customizable chart types [i.e. data views] to suit individual preferences. ➢ flexibility to set multiple, meaningful RTM threshold alarms.
SIMPLE, INTUITIVE AND EASY-TO-USE.	

SDS, a company that has been delivering mainframe software for over 23 years, has gone to great lengths to ensure that its *new* **VITALSIGNS for IP (VIP) v4** meets all of the above iterated characteristics for

a good, incisive and easy-to-use mainframe TCP/IP network monitor. Focusing on simplicity to overcome much of the inherent complexities of mainframe TCP/IP networking has been an overriding design goal of VIP – from day one. It thus sets out to define a new standard for fast, comprehensive, browser-based, graphical TCP/IP monitoring that emphasizes simplicity, clarity and flexibility. It eliminates *blind spots* [e.g. a server that is hung or under stress] that are possible with other schemes, and v4 now offers a state-of-the-art RTM facility for tn3270 traffic using mainframe resident tn3270 servers.

VIP uses an agent/server architecture, with VIP monitoring agents available for OS/390 v2.9 all the way through to z/OS v1.6. Data gathered by the agents are fed, in real-time, to one or more VIP servers *[with the agents making sure that only the data that has changed is sent to the servers so as to minimize agent-server traffic]*. Deploying multiple servers guarantees resilience for *'zero downtime'* operations. The VIP servers, which are implemented in JAVA, can be deployed on PCs running Windows, Linux/Unix servers [including Linux LPARs], or an 'MVS' LPAR with Unix System Services (USS).



THE LOW-OVERHEAD, FLEXIBLE AGENT/SERVER ARCHITECTURE OF VIP V4 WITH ITS ABILITY TO MONITOR MULTIPLE LPARS ON MULTIPLE MAINFRAMES FROM A SINGLE BROWSER-BASED SCREEN AND DELIVERS FAULT-TOLERANT CONFIGURATIONS THROUGH THE USE OF REDUNDANT VIP SERVERS.

VIP v4: Fifteen (15) Clear Differentiating Features

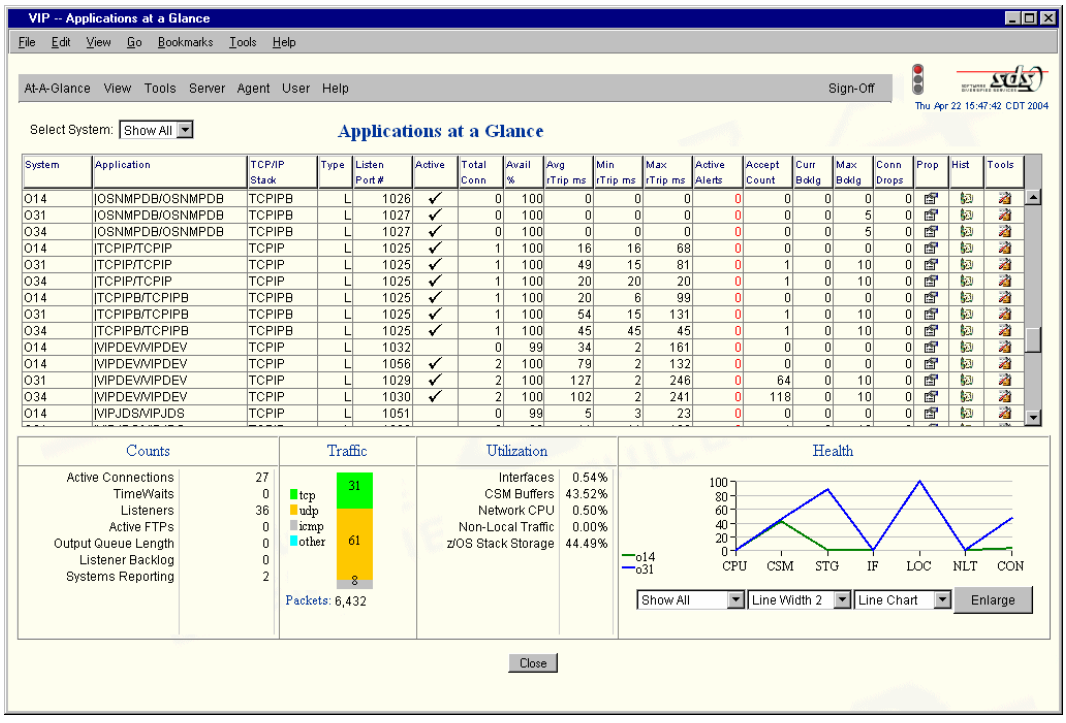
1. Direct retrieval of all necessary management data from the pertinent TCP/IP stacks using a cross-memory interface -- obviating the need for repetitive, inefficient SNMP queries, high-overhead packet tracing, or ungainly 'screen scraping'.

2. Stack access for management data augmented by full SNMP support to provide visibility of remote hosts [e.g. routers] and Linux LPARs, so as to eliminate any and all 'blind spots' within the network.

3. Browser-based GUI that permits an entire network, consisting of multiple systems and multiple LPARs, to be viewed and monitored from within a *single window*.

4. Truly real-time alert handling to facilitate anticipatory management.

5. Comprehensive and flexible, RFC 2562 standard-based response time monitor (RTM) for tn3270 traffic using mainframe-resident tn3270(E) servers, that is capable of monitoring an entire server, a specific subnet or individual sessions -- with the response times, furthermore, split into their SNA system versus IP network transit time sub-components for a thorough understanding of end-to-end performance characteristics and potential bottlenecks.



The "Applications at a Glance" screen from VIP v4 illustrating its trademark browser-based graphical screen presentation.

6. Detailed visibility of OSA(-Express) operations, at a glance, for both TCP/IP and SNA traffic, including operational status, actual data transfer speeds, LPAR utilization and traffic activity – with the option of *'drill down'* analysis on each entry.

7. Fast, automatic, dynamic discovery of stacks, applications and interfaces -- on a continual basis, so as to transparently accommodate LPAR or stack reactivations.

8. Easy access to statistics from z/OS COMM. SERVER about INTRUSION DETECTION SERVICES (IDS) status for TCP/IP stacks.

9. Powerful remote host monitoring capability that provides in-depth visibility of remote hosts outside the mainframe, replete with features such as PING response time recording, path length measurement, connection statistics and stress testing options.

10. Ability to activate multiple Response Time Monitors (RTMs), on-demand or via scheduled automated activation, to monitor multiple servers, or various permutations of subnets and individual sessions with the option of setting various meaningful thresholds values for generating alerts on any unexpected deviations in response time characteristics within customizable sample periods.

11. Provides 9 incisive, at a glance, network monitoring screen interfaces (all of which can be customized to display the data in different views) for:

- NETWORK STATUS	- ALERTS	- APPLICATIONS
- FTP	- TELNET/TN3270(E)	- EE
- NETWORK ACTIVITY	- OSA	- REMOTE HOSTS

12. Includes 8 powerful and utilitarian (but easy to use) diagnostic tools that address all pertinent TCP/IP network management scenarios:

- PING (ICMP & UDP)	- IP PACKET TRACE	- DNS LOOKUP
- TRACEROUTE	- SNMP MIB QUERIES	- CHRONOLOGY LOG
- CONNECTIONS EXPLORER	- MVS SYSTEM OPERATOR COMMAND CONSOLE	

13. Fault-tolerant, *'zero downtime'* configurations possible, at very low costs, through the use of redundant VIP servers.

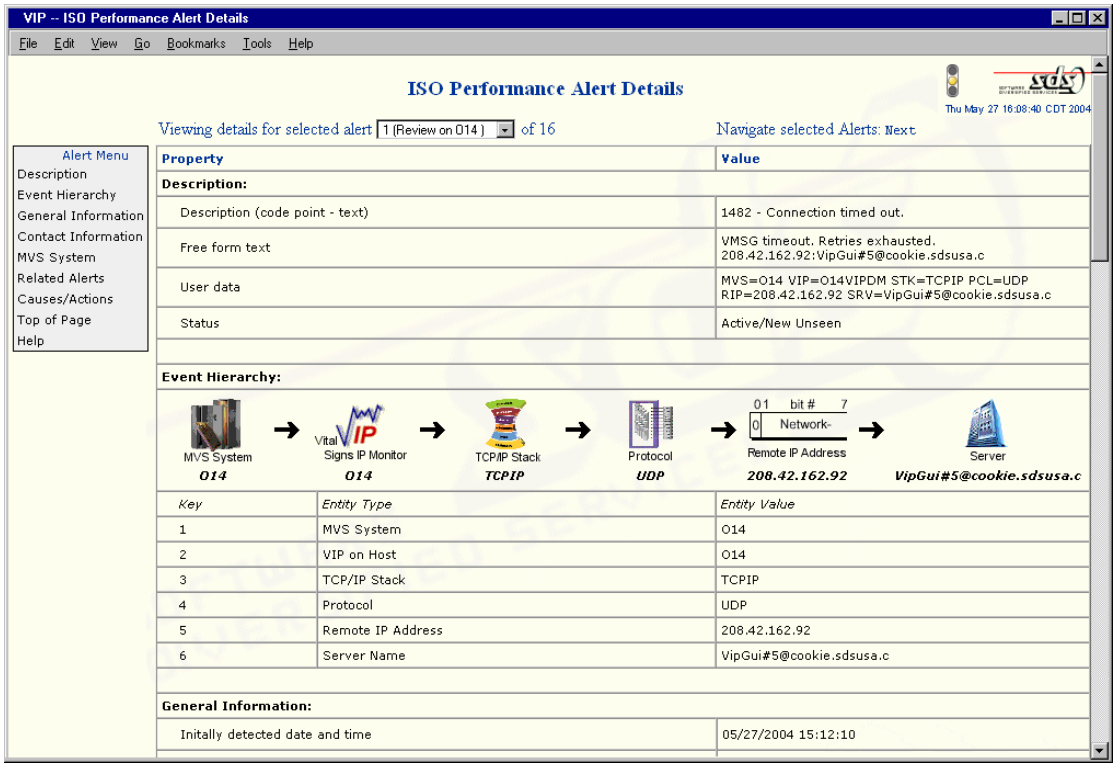
14. A full, successful installation is unlikely to take more than one hour.

15. Superior documentation and exceptional technical support from SDS.

The above list of 15 items, though persuasive on its own, is by no means the only differentiating features possessed by VIP v4. VIP v4 includes many, many more, such as:

- extensive tracking of FTP session activity
- activity at a glance, sorted by system, on a system/stack, stack/application basis, with multiple, dual-field based ranking options
- 'Telnet At A Glance' linkage with the tn3270 RTM to provide easy access to Telnet LU Groups and server data -- thus enabling quick retrieval of inactive LUs or further analysis of RTM thresholds to determine the need for additional response time monitoring to spot potential 'trouble spots'
- TCP connection activation/deactivation monitoring using SMF EXITS
- packet traces maintained in IPCS format for compatibility with IBM's packet trace utility, with optional conversion for use with SNIFFERs
- alert forwarding to NETVIEW via a program-to-program interface (PPI)
- COMMON STORAGE MANAGER (CSM) statistics
- EE connection data

To exhaustively go through the complete list of VIP v4 differentiators is not, however, a goal of this white paper. This white paper instead wishes to focus on a few specific VIP v4 highlights. You should contact SDS for other collateral that will list all of VIP v4's capabilities.



ALERTS DETAIL SCREEN

VIP v4: The Architecture is the Key

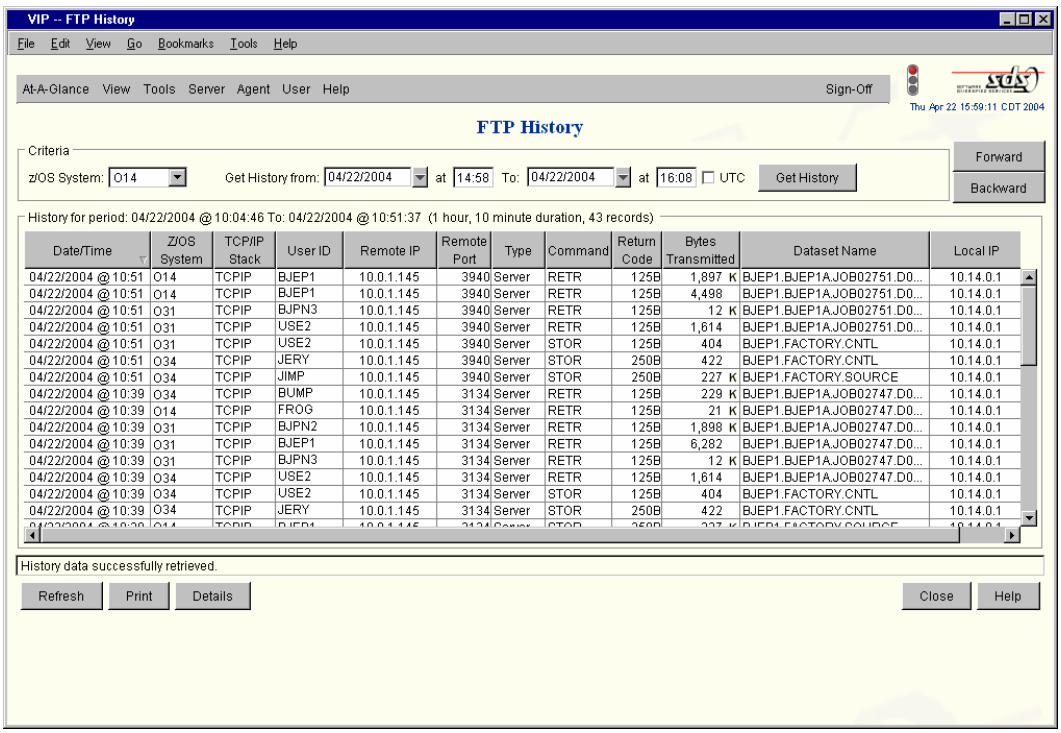
Mainframe professionals, more than most, understand and appreciate the power and long-term benefits of having products built around a sound and solid architecture. They know about mainframe POPs and SNA. Having been a mainframe shop for over two decades, SDS valued the manifold benefits of well architected software solutions. Hence they went to great lengths to ensure that VIP was to be built per the dictates of a well reasoned and carefully thought out architecture.

The core architectural requirements for VIP revolved around efficiency, functionality, reliability, and extensibility – all of it tempered, throughout, with simplicity. The resulting architecture, that has been repeatedly validated and vindicated, over the last few years with VIP v1, v2 and v3, consists of three primary methodologies:

1. direct data collection from the TCP/IP stacks using a variety of APIs, to gather as much data as possible directly from the source, rather than relying exclusively just on SNMP, packet interception, or screen scraping – though VIP does use SNMP and packet tracing to augment the data it extracts directly from the TCP/IP stacks.

2. reliance on a flexible, unrestricted VIP agent/VIP server configuration which permits the use of multiple servers, and the ability for VIP agents to simultaneously forward *(modified)* data to multiple VIP servers [as shown in the figure on page 7].

3. browser-based, highly graphical data presentation scheme.



FTP History Screen

Each of the above chosen methodologies has its own set of unique advantages. For example, VIP being browser accessible means that *suitably authorized* system operators can monitor and manage their TCP/IP network from anywhere in the world – whether it be another building, a conference room, home, hotel, airport lounge, or a health club. But that is not all.

These three methodologies together, provide VIP with significant synergy relative to its core design goals. These can be summarized as follows:

	Direct Stack Access	Agent/Server	Browser-based
Efficiency	✓	✓	✓
Speed	✓	✓	
Low mainframe usage	✓	✓	✓
Functionality	✓	✓	✓
Extensibility	✓	✓	✓
Reliability/Redundancy		✓	✓
Overall Simplicity	✓	✓	✓
Ease-of-Use			✓
Fast Installation	✓	✓	✓

Direct TCP/IP Stack Access: A Noteworthy Breakthrough

The significance and implications of VIP's direct TCP/IP stack access scheme for management data harvesting are huge – and far reaching. It was an inspired and breakthrough design decision that enables VIP to outclass competitive offerings on multiple fronts.

If you stop and think about it, even for a second, it is easy to see that all TCP/IP related data maintained by a MIB must come, in the first place, from, or via, the TCP/IP stack. This is the basic premise of what this key VIP feature is all about. *If you can tap into the required data at its very source, i.e. the stack, then there is really no rationale for using any other scheme*.

VIP's direct stack access scheme allows it to retrieve all the same TCP/IP monitoring data that SNMP obtains from the standard TCP/IP and IBM Enterprise MIBs – *albeit at a fraction of the processing overhead*. This translates directly to:

- ❖ speed
- ❖ responsiveness
- ❖ low CPU utilization

With this approach you get genuinely real-time, minimally obtrusive network monitoring that does not get in the way of the production workloads that it is supposed to be monitoring. In reality, direct stack access, à la VIP, is the best way to obtain accurate real-time data about TCP/IP activity.

AVOIDING THE SNMP TRAP FOR STACKS

The SNMP approach for obtaining mainframe MIB data, the technique used by the other competitive mainframe monitors, can be extremely inefficient and cumbersome – with no redeeming merits. To use SNMP, one needs to configure and activate the OSNMP daemon – for each stack that needs to be monitored. There are processor overhead and administrative costs involved with just setting up and maintaining these daemons.

Once configured and activated, the daemon for each stack has to be repeatedly polled, via UDP packets, to obtain the necessary data from the MIBs. In some cases, these queries to the OSNMP daemon can result in large amounts of superfluous data, such as lengthy connection tables. These repeated polls, and the data they generate, consume considerable mainframe bandwidth and furthermore impinges on the processing of the production workload. Genuine, real-time network monitoring is really not possible with this approach.

Much of the pertinent data available via this high-overhead daemon querying technique is available to VIP via an efficient, IBM provided API that works on a cross-memory basis between the stack and the VIP agent. Rather than receiving superfluous data, VIP can get exactly what it wants, from the stack – *when it needs it*. VIP's direct stack access scheme is thus a win-win proposition. It provides VIP with much of the information it needs at a fraction of the overhead associated with the SNMP approach. This is why VIP v4, like the previous versions of VIP, is noted for its low CPU usage, while competing products are known to require 5% or more.

The bottom line here is that one cannot escape the fact that the SNMP approach is inferior to the direct, cross-memory stack access scheme used by VIP v4 – whichever way you try to slice or dice it. One can sum it up in one pithy phrase:

When it comes to mainframe TCP/IP, SNMP is just passé.

USING SNMP FOR REMOTE HOSTS

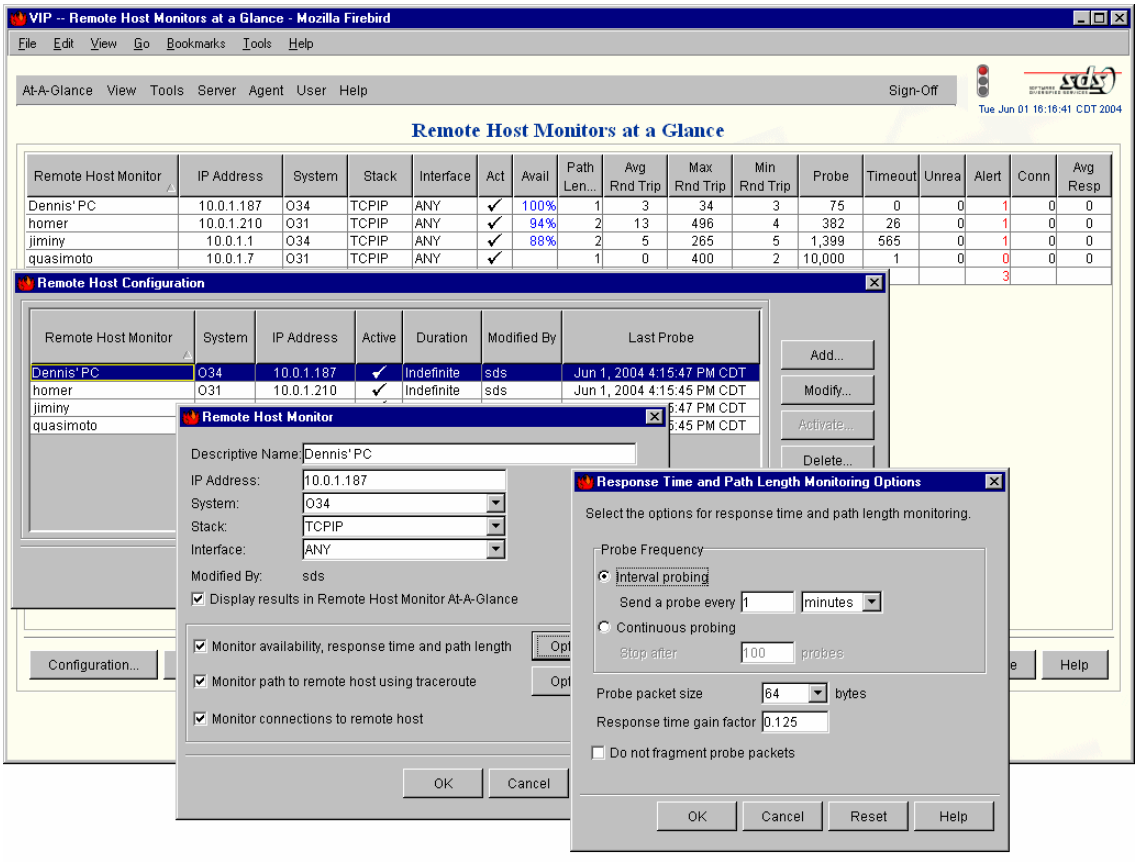
Just because VIP v4 eschews SNMP for getting mainframe TCP/IP stack data does not, however, mean that VIP v4 does not support SNMP. In reality, VIP v4 includes uncompromised SNMP support.

The VIP v4 SNMP MIB inquiry capability, moreover, supports the mandatory product MIB, IBM's enterprise MIB and the OSA MIB.

This SNMP support, augmented by PING and traceroute, form the core of VIP v4's powerful remote host monitoring capability (as was also the case with VIP v3). Thus with VIP v4 you get the best of both worlds – SNMP-based monitoring when you need it, and direct stack access when using SNMP does not make sense.

*This **unique**, dual 'feed' approach of using both direct stack access and SNMP in tandem is important to keep in mind when evaluating VIP v4.*

The bottom line is that VIP v4 includes comprehensive, undiluted, standards-compliant SNMP support. However, VIP does not use SNMP in situations where it can much more efficiently get the data it needs directly from a stack.



VIP V4: REMOTE HOST MONITORING

THE FUTILITY OF RELYING PRIMARILY ON PACKET TRACING

TCP/IP monitoring products that rely primarily on packet tracking as opposed to SNMP may also be inefficient and result in high-overhead. In fact, packet tracing misses out on certain critical data, such as IDS activity, that is however, always available to VIP v4 from the stack.

Furthermore, packet tracing can result in dangerous blind spots! For instance, a mainframe that is hung [i.e. not responding] or is under undue stress may be indicated by an unexpected rise in the current connection backlog, especially if it is starting to approach the maximum backlog threshold. When this backlog threshold is exceeded, the mainframe begins to start quietly dropping new connection requests, per the accepted conventions of IP networking.

A packet trace scheme because it only sees the packets, and cannot see the backlog values maintained between TCP and the application, is unable to raise an alert *before* the mainframe starts dropping connections. That is a huge blind spot. *Not so with VIP v4*. Because VIP v4 monitors the connection backlog statistics at the stack, it can generate an alert before a mainframe starts dropping connections.

Packet tracing is meant to be a diagnostic tool. *It is not meant to be used as the primary means of network monitoring.*

Packet tracing involves intercepting and then analyzing each and every packet destined to, or originating from, a TCP/IP stack. It involves copying and storing packet images so that they can be processed to extract the relevant networking monitoring related data. Though, at face value, this approach may appear to be a viable means of providing real-time network monitoring, in reality, it is fraught with drawbacks.

For a start, just the act of intercepting and copying all packets slows down all network traffic! Mainframe performance experts will vouch for this. The delay introduced by packet tracing is such that in some cases timing related TCP/IP problems can be "fixed" by activating packet tracing to slow down the network traffic. So packet tracing rather than being truly real-time, instead distorts real-time network processing.

This technique, with its reliance on data copying, may also incur significant CPU, virtual storage and paging overhead. The bottom line here is that just as with SNMP MIB querying, packet tracing is not a method suited for fast, low-overhead mainframe TCP/IP monitoring.

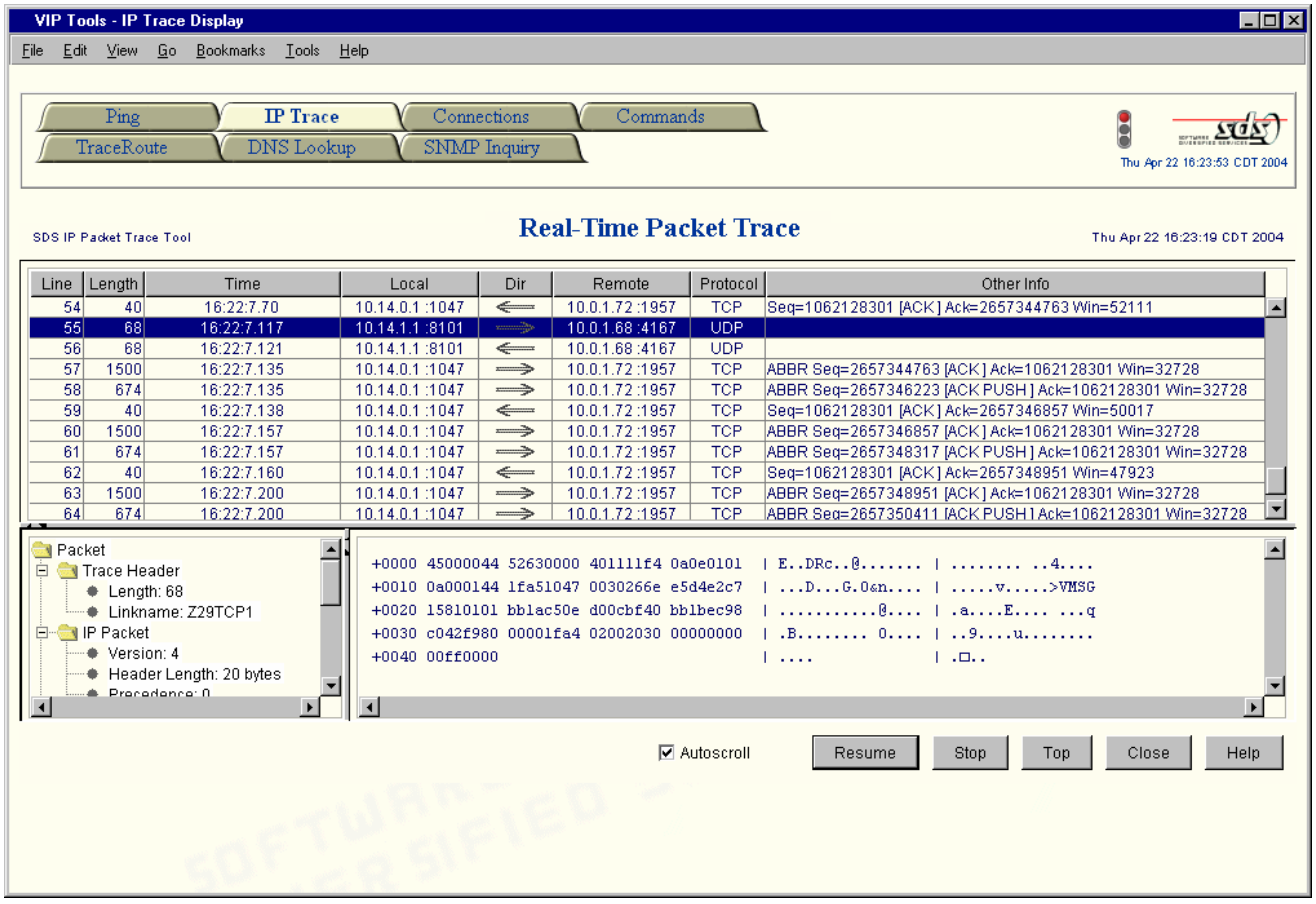
Packet tracing, though not optimum for network monitoring, is, however, a very useful diagnostic tool for problem isolation. Thus, just as with SNMP, VIP v4, does indeed have a powerful IP packet trace facility that interfaces

directly to IBM's packet trace utility. In addition, VIP v4's incisive and flexible tn3270 RTM features does use packet tracing -- albeit just for the packets associated with the tn3270 sessions being monitored. This is another example, as with the SNMP support, of VIP making sure that customers always get the best of all worlds; packet tracing for diagnostic purposes as well as tn3270 RTM, and direct stack access for monitoring.

WRAPPING UP DIRECT TCP/IP STACK ACCESS

It should be clear by now that the VIP v4 approach of obtaining the data necessary for incisive TCP/IP monitoring directly from the relevant stack is the best approach for real-time, low-overhead operation. It does not have the limitations associated with SNMP-based MIB queries, packet tracing, or screen scraping, z/OS TCP/IP stacks contain a wealth of pertinent statistics. *For example, the z/OS stack maintains 43 separate performance statistics just for TCP traffic.*

Thus VIP v4's rationale for opting for direct stack access, rather than using SNMP or packet tracing, is obvious and extremely logical. The stack is the source of most of the data required for incisive, real-time mainframe TCP/IP monitoring.



VIP V4 PROVIDES A POWERFUL REAL-TIME PACKET TRACING CAPABILITY AS A DIAGNOSTIC TOOL.

TN3270 RESPONSE TIME MONITORING (RTM): ADDING LONG-RANGE RADAR TO SEE BEYOND THE HORIZON

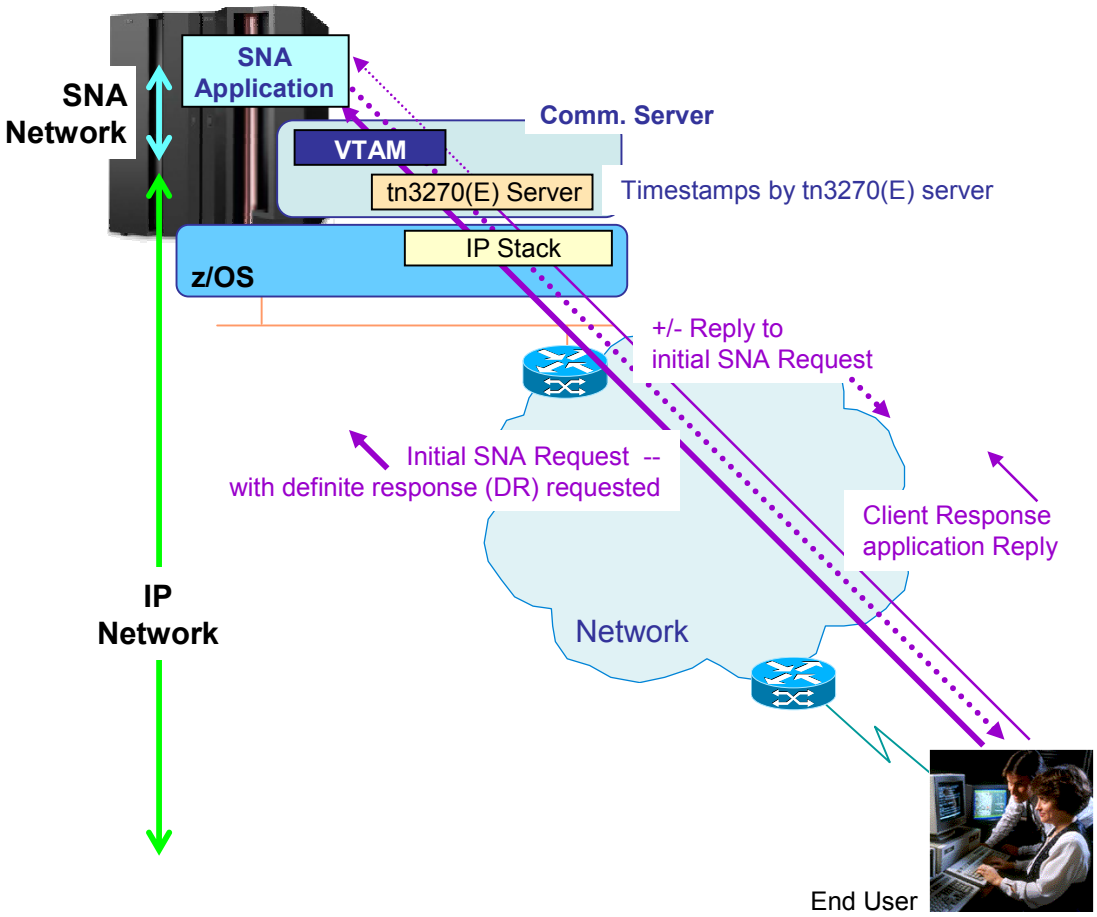
An incisive and flexible tn3270 RTM scheme, based on RFC 2562[1], is a key new feature of VIP v4. Intelligent monitoring of tn3270 response times with multiple threshold settings, with any unexpected deviations automatically generating an alarm, tends to be a critical, and very accurate, measure of overall system/network health and stability. Seasoned network administrators know that any sudden swings in response time characteristics tend to be a leading-edge indicator that something has changed within the overall system.

An increase in tn3270 response times would typically signal either a failure of a interface, rerouting within the IP network, growing congestion at one or more nodes, an application failure being compensated for by a Parallel Sysplex setup, or intermittent errors on a network link. A sudden, unexpected decrease in tn3270 response times, as mentioned earlier, could also be an indication that something has changed within the system/network – thus providing the 3270 traffic with more bandwidth (or system resources. A incisive RTM scheme is thus, indubitably, a sound and unparalleled 'early warning' system vis-à-vis system/network management.

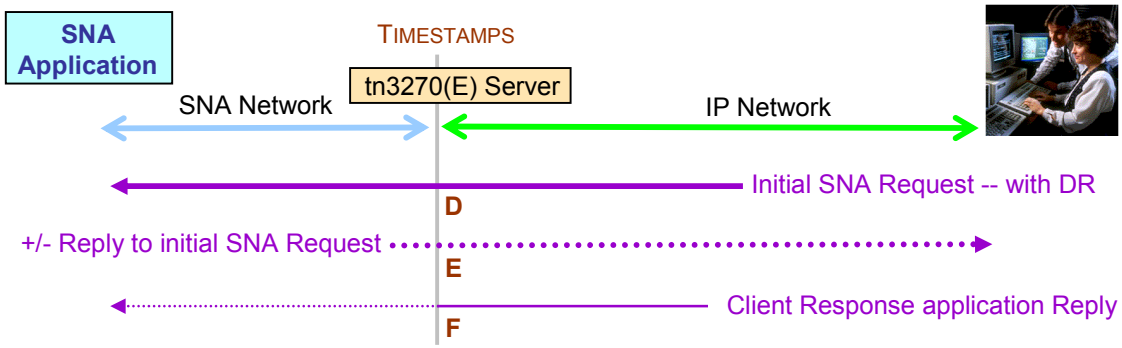
The VIP v4's RTM scheme is powerful and flexible with no artificial caveats. The v4 RTM is capable of monitoring an entire server, a specific subnet or individual sessions. It is also possible to have multiple RTMs, with each RTM invoked on-demand or via a pre-scheduled automated activation. When multiple RTMs are being used, VIP permits overlap in terms of what each is monitoring. Thus it is indeed possible to have two RTMs monitoring subnets with overlapping connection 'pools', or to have one monitoring a subnet while the other is monitoring the entire server. The bottom line here is that VIP v4 comprehensively (and easily) addresses all customer requirements when it comes to RTM.

The v4 RTM can be used monitor response times to a specific remote location, determine the validity of a user complaining of slow performance, check the 'health' of a specific tn3270(E) server, or provide detailed, historic data for resolving 'service-level agreement' (SLA) disputes. VIP also permits the tn3270 RTM data to be easily correlated with the 'Telnet At A Glance' data to enable quick access to Telnet LU Groups and server data. It also permits response times to be split into their SNA system versus IP network transit time sub-components.

[1] *"Definitions of Protocol and Managed Objects for TN3270E Response Time Collection Using SMIv2 (TN3270E-RT-MIB)"* submitted by IBM in April 1999.



Detailed depiction of the configuration and SNA message flows involved in tn3270(E) RTM per RFC 2562. *A simplified scheme of this configuration showing the timestamps used by RTM is shown below.*

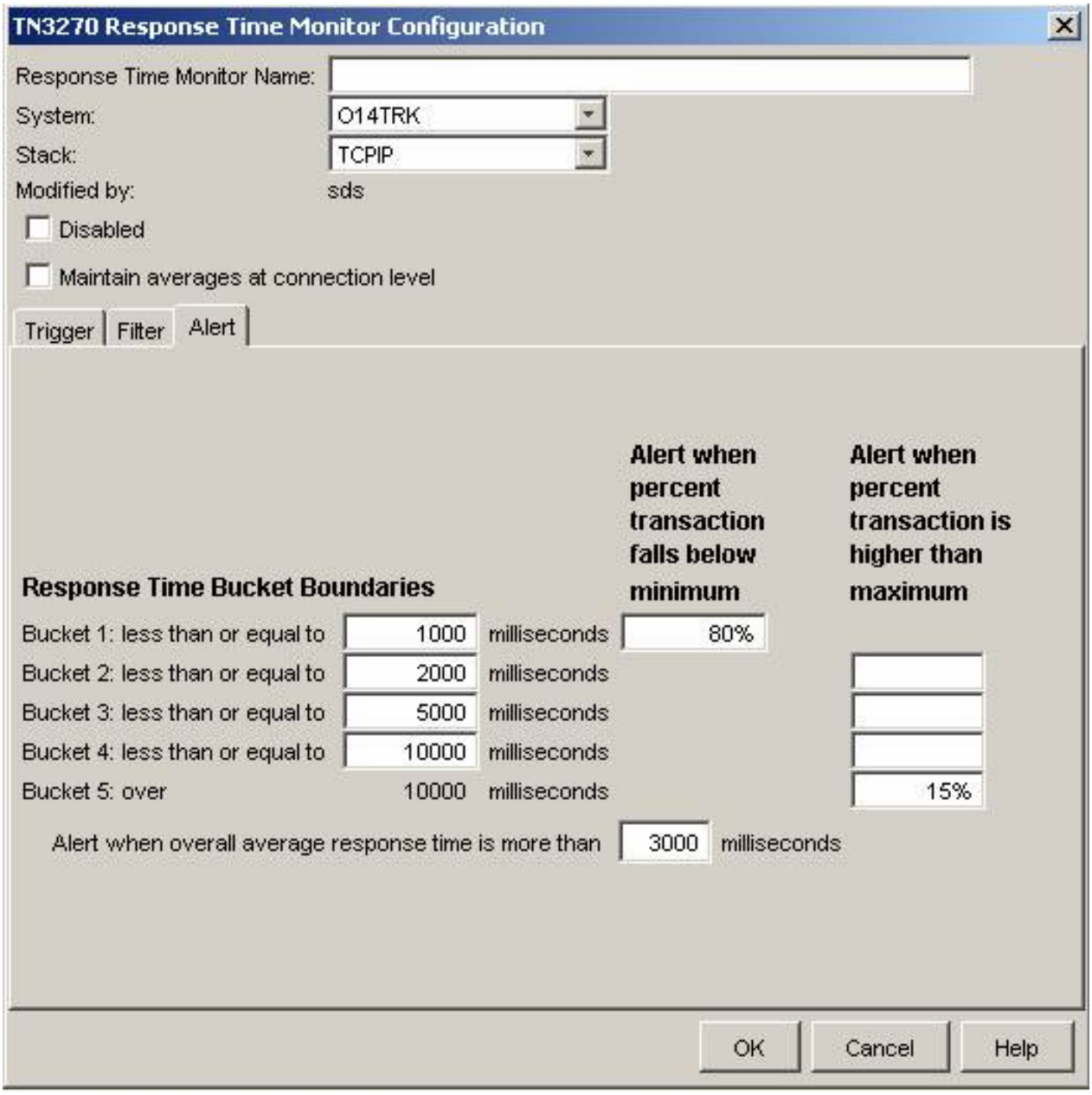


Total Response Time = Timestamp "F" – Timestamp "D"

IP Network Transit Time = Timestamp "F" – Timestamp "E"

The VIP v4 RTM enables network administrators to define five response time "buckets" for "Total Response Time" and "IP Network Response Time" [see diagram above] – for each monitor that is being used. These RTM thresholds and boundaries, as previously discussed, serve as extremely accurate 'early warning' alert criteria.

With VIP it is possible to set these thresholds on a 'cumulative' basis in terms of generating an automated alarm. So it is possible to specify that an alarm should be raised if less than 80% of transactions fell into bucket 1, or more than 5% of transactions fell into bucket 4, or the overall average response time threshold time exceeds the predefined threshold. [Refer to the RTM Configuration screen shown below to see how easy this is to setup.] And remember it is possible to have multiple RTMs – monitoring overlapping 'entities', if need be, each with monitor working having its own specific set of threshold values.



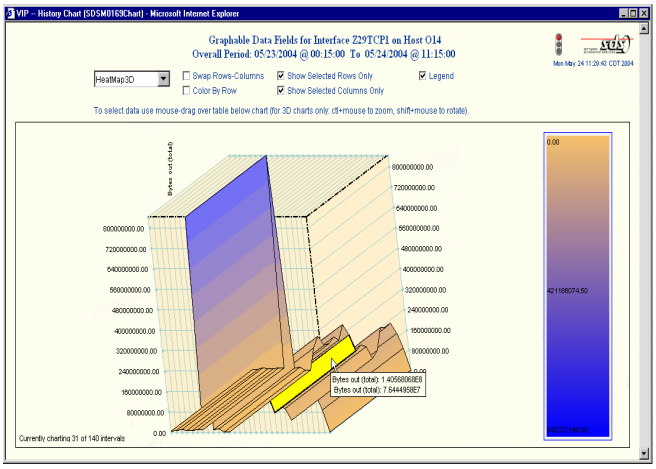
VIP V4 TN3270 RTM CONFIGURATION SCREEN SHOWING HOW THE RESPONSE TIME THRESHOLD BUCKET BOUNDARIES ARE SPECIFIED.

DATA PRESENTATION: MAKING SENSE OF IT ALL

Albert Einstein, who knew a thing or two about what true knowledge is all about, was fond of observing that:

"INFORMATION IS NOT KNOWLEDGE"

Raw network management data, presented haphazardly, will not help you get a handle on what is really happening on a mainframe network. The network management information, whether obtained from a stack, SNMP, a Ping, or an IP packet trace, has to be presented to the operator in ways which makes immediate sense – at a glance.



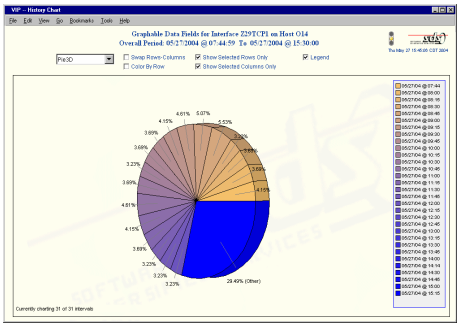
Contemporary mainframe networking, fueled by gigabit interfaces and the increasingly more powerful zSeries processors, continues to get faster and busier. Dramatic changes within the network can occur in split seconds. System operators must have all the information they need – at once, on one screen, and in a manner that allows them to make quick decisions.

Operators do not have the time to wade through multiple, disparate screens searching for the information they need. Ideally they have to have all the pertinent information consolidated, summarized and highlighted, in a single meaningful view – with, of course, the option of being able to quickly drill down into progressively more detailed views on the click of a button.

In order to be useful, a mainframe TCP/IP monitor, at a minimum, must offer the following data presentation capabilities:

- centralized view of the whole network – encompassing multiple LPARs per system in a multi-system configuration.
- at a glance summaries of all pertinent entities, including the network, alerts, applications, FTP, telnet/tn3270(E), Enterprise Extender, OSA(-Express) adapters, and remote hosts – with attention focusing color coded icons and semaphores for alerts.

- fast, point-and-click navigation – with consistency across all screens.
- detailed views on-demand.
- graphical data selection tools, such as drop down 'month at a time' calendars, to expedite option specification.
- equal access to both real-time and historic data, particularly for FTP and telnet/tn3270(E) traffic.
- multiple customizable views to accommodate individual or corporate preferences.
- crisp and consistent responsiveness to keep pace with operator demands.



Browser-based, highly graphical data presentation, as discussed earlier, is another stand-out feature of the VIP v4 architecture. Suffice, at this juncture, just to say that VIP v4 offers all of the data presentation capabilities mentioned above – plus a lot more.

VIP v4, thus, does not present operators with just a torrent of raw data, or a very narrow, specific view of a network subcomponent [e.g. a single stack or a single application]. Instead VIP v4 gives you the total, big picture, at a glance, with the necessary views and tools to drill down to progressively more detailed views – as needed. Yet another instance of VIP v4 giving users the best of all worlds.

BUILT-IN ADVANTAGES OF A BROWSER-BASED APPROACH

The Web browser is destined to become the universal user interface. IBM, for one, is an avid advocate of this, and has been since 1997. IBM's strategic WebSphere Host On-Demand and Host Publisher offerings for mainframe application access, both of which are browser-based, demonstrates IBM's belief that all future application and data access should be via a standard Web browser – rather than through proprietary GUIs.

A browser-based GUI, as implemented by VIP v4, has many, automatic, built-in advantages. Key among these being:

- operator familiarity.
- mobility – i.e. authorized access from anywhere across an intranet, extranet, or the Web.

- guaranteed platform independence across Windows, Linux and Unix.
- interface and navigational consistency.
- seamless support for Java.
- ability to easily maintain multiple, separate browser instances per workstation.
- straightforward internationalization.
- standardized upgrade policies and procedures.
- proven stability.

The bottom line here is that VIP v4 with its browser-based GUI sets out to define a new and compelling standard for mainframe TCP/IP monitoring. The best way to appreciate the value of this interface is to look at an on-line demo, or better still to actually test drive a VIP v4 installation.

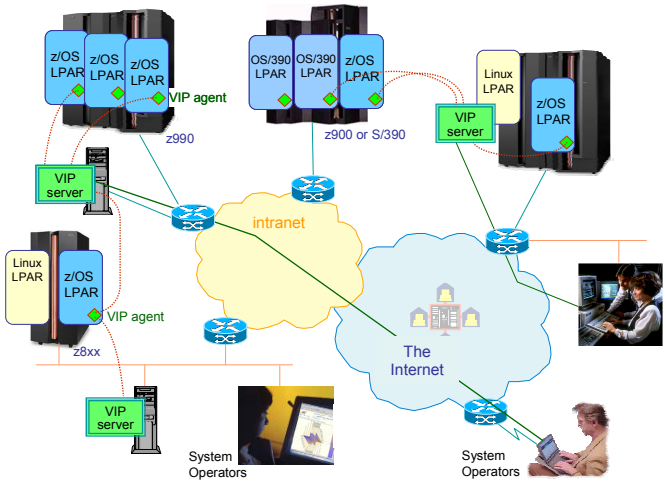
AGENT/SERVER ARCHITECTURE

The agent/server architecture used by VIP v4 results in:

- very low mainframe CPU utilization.
- seamless accommodation of multi-LPAR, multi-mainframe networks.
- the option to easily realize redundant, fault-tolerant configurations for 'zero downtime' operations.
- the ability to quickly and easily add LPARs or mainframes to an existing network.
- *low cost deployments* given that VIP servers can be implemented on PCs running Windows or Linux.
- the option of being able to affordably, and non-disruptively, upgrade the platform on which a VIP server is deployed, without in anyway impacting mainframe operations.
- the *offloading* of network monitoring related data processing, data analysis and data presentation functions so that these functions do not get in the way of mainframe production workload processing.

The VIP monitoring agents are written in optimized ASSEMBLER for maximum speed and efficiency. VIP agents are currently available for OS/390 v2.9 all the way through to z/OS v1.6. It is these agents that access the mainframe TCP/IP stacks for management data, or interface with IBM's packet trace utility for IP packet traces.

New [i.e. modified] data gathered by the agents are fed, in real-time, to one or more VIP servers. The use of multiple servers ensures resilience for *'zero downtime'* operations. The VIP servers, which are implemented in JAVA, can be deployed on PCs running Windows, Linux/Unix servers [including Linux LPARs], or a 'MVS' LPAR with Unix System Services (USS). The ability to have the VIP servers on non-mainframe platforms enables customers to offload network management functions from the mainframe – thus freeing up CPU cycles for more production work.



VIP v4: THE BOTTOM LINE

VIP v4 sets out to simplify mainframe TCP/IP monitoring. It has been thoughtfully architected to be fast, comprehensive, low-overhead, reliable and easy-to-use. It uses a flexible, agent/server configuration that supports redundancy as well as low-cost server platforms. VIP v4, in addition, includes an incisive and flexible tn3270 RTM scheme that permits multiple overlapping monitors.

It, in marked contrast to other offerings, has no blind spots [e.g. rising connection backlogs] vis-à-vis mainframe TCP/IP networks. VIP v4 precludes the dangers of *"flying blind"* when it comes to TCP/IP networking, while the new RTM capability is akin to getting a long-range radar system for overall system/network health and stability.

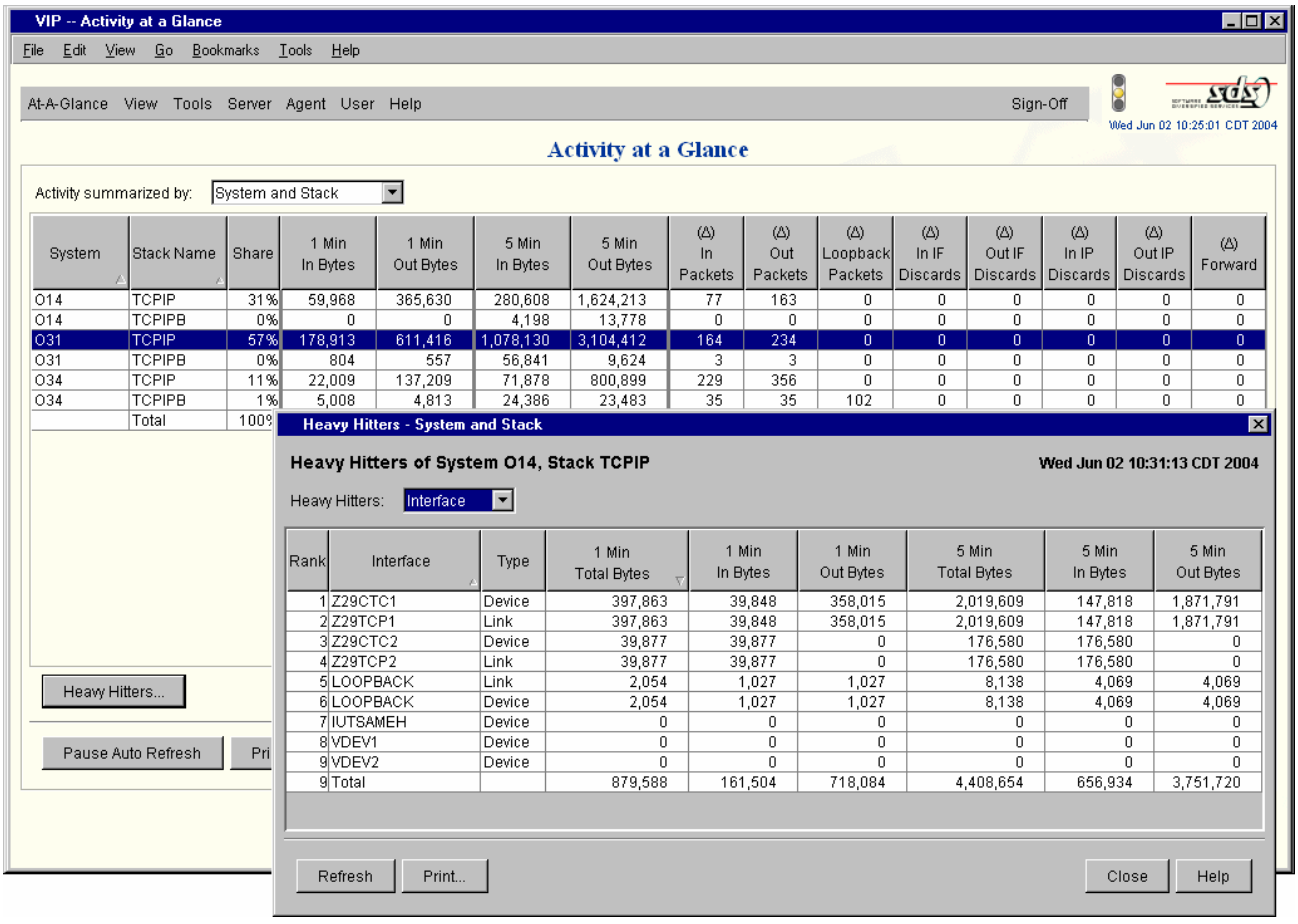
Unlike most of other mainframe monitors it does not rely on SNMP MIB queries, packet tracing or screen scraping, which are all known to be inefficient and cumbersome, for its primary data collection needs. VIP v4, instead, directly accesses the relevant z/OS TCP/IP stacks, via a cross-memory interface, to obtain most of the network management data it requires. As a result VIP v4 provides true real-time network monitoring, at a fraction of the mainframe CPU utilization used by other offerings. VIP v4 offers incisive support for FTP, telnet/tn3270(E), Enterprise Extender (EE), OSA(-Express) and remote hosts [i.e. routers]. Where appropriate [e.g. FTP and telnet/tn3270(E)] it maintains detailed historic logs that can be searched for past activity.

Though opting not to use SNMP or packet tracing for its vital network monitoring functions, VIP v4, nonetheless, includes uncompromised support for SNMP as well as IP packet tracing for diagnostic purposes and

RTM. It also has support for PING, DNS lookup and route tracing, not to mention a standard MVS system operator command console.

A highly-graphical, browser-based operator interface, with multiple at a glance views, is a trademark of VIP v4. This carefully designed 'point-and-click' interface, with color coded icons and built-in data selection tools, is intuitive, compelling, easy-to-learn – and easy-to-use. It is also customizable. This interface never gets in the way of what an operator is trying to achieve.

VIP v4 is, indubitably, the way to master the growing complexity of mainframe networking and monitor tn3270 response times. With VIP v4 you can indeed have a 'zero downtime' mainframe TCP/IP network with high-performance to boot.



VIP'S ACTIVITY AT A GLANCE SCREEN.

SELECTED GLOSSARY

browser	Web browser such as Internet Explorer (IE)
Enterprise Extender	end-to-end, mainframe-to-client, SNA transport across an IP network using HPR
HPR	the final iteration of SNA and APPN, essentially representing APPN+
HiperSockets	TCP/IP-based, inter-LPAR communications scheme
MIB	management information base, a database of network management objects for a given entity
RTM	Response Time Monitor for tn3270 traffic
SNMP	set of TCP/IP-centric network management protocols
stack	software implementation of the TCP/IP protocol within a system (or LPAR)
telnet	TCP/IP-based terminal protocol for application access
tn3270(E)	3270 specific variant of telnet that works on a client-server basis
VIPA	virtual IP address, *akin to an alias*, assigned to a mainframe IP resource [e.g. stack, OSA interface, TCP/IP application], to facilitate fault-tolerance and resource movement by masking the actual IP addresses of resources from external entities
VIPA Takeover	automated recovery of TCP/IP resources in a sysplex by the transfer of virtual addresses
Web-to-host	browser-invoked host access schemes

SOFTWARE DIVERSIFIED SERVICES

Software Diversified Services (SDS), [www.sdsusa.com] based in Minneapolis, MN, has been providing premium mainframe solutions to the IBM world since 1981. It currently has in excess of 1,500 mainframe customers worldwide.

SDS' mainframe product repertoire now includes over twenty MVS, VM and VSE products, with VIP v4 being one of these. SDS also markets PC software related to mainframe operations. The products marketed by SDS focus on network management, performance monitoring, report distribution, data compression, terminal emulation, and client-server applications.

SDS is noted for having the highest quality software, documentation, and technical support in this industry sector. SDS technical support has been rated #1 by the prestigious IBEX Bulletin.

THE AUTHOR: ANURA GURUGÉ

Anura Gurugé [www.guruge.com] is an ex-IBMer (at Hursley, UK) from the 1970s. In addition to being a systems programmer he was involved with the 3270 program. His 1st book, *"SNA: Theory and Practice"* [which is still in print] was published in 1984, five years after he left IBM. For the next 15 years he was "Mr. SNA", and was heavily involved with Token-Ring switching, Frame Relay and Web-to-host. He was associated with the Token-Ring switching pioneer Nashoba Networks, which was acquired by Cisco Systems.

These days he is a consultant, a teacher, and writer. He is the Editor at Large for *"IT In-Depth"* [www.itindepth.com], as well as the new *"Enterprise Open Systems Journal"*. He also writes the "Deep Blue" column for z/Journal. He is also the author of four other books, with his latest being "Web Services: Theory and Practice". In addition, he has published over 350 articles. In a career spanning 30 years, he has held senior technical and marketing roles in IBM, ITT, Northern Telecom, Wang and BBN. He can be contacted at (603) 455-0901 or anu@guruge.com.

SOFTWARE DIVERSIFIED SERVICES
6010 EARLE BROWN DRIVE
BROOKLYN CENTER, MN 55430

PHONE: 763-571-9000
FAX: 763-572-1721

WWW.SDSUSA.COM