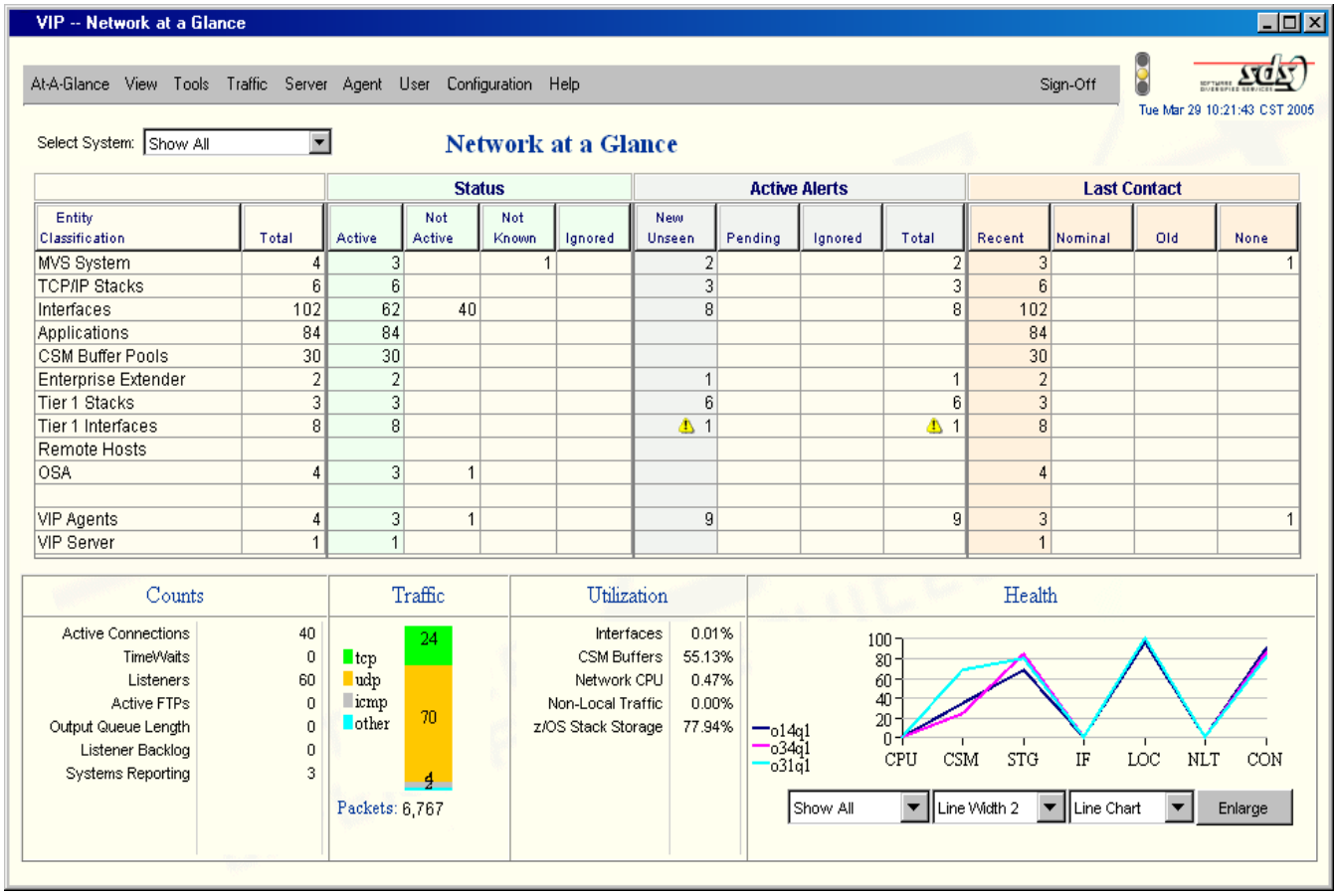
Mainframe TCP/IP Problem Resolution, in Real-Time, with SDS VIP v4

Software Diversified Services (SDS)

VitalSigns for IP

Proactive, anticipatory management

A White Paper

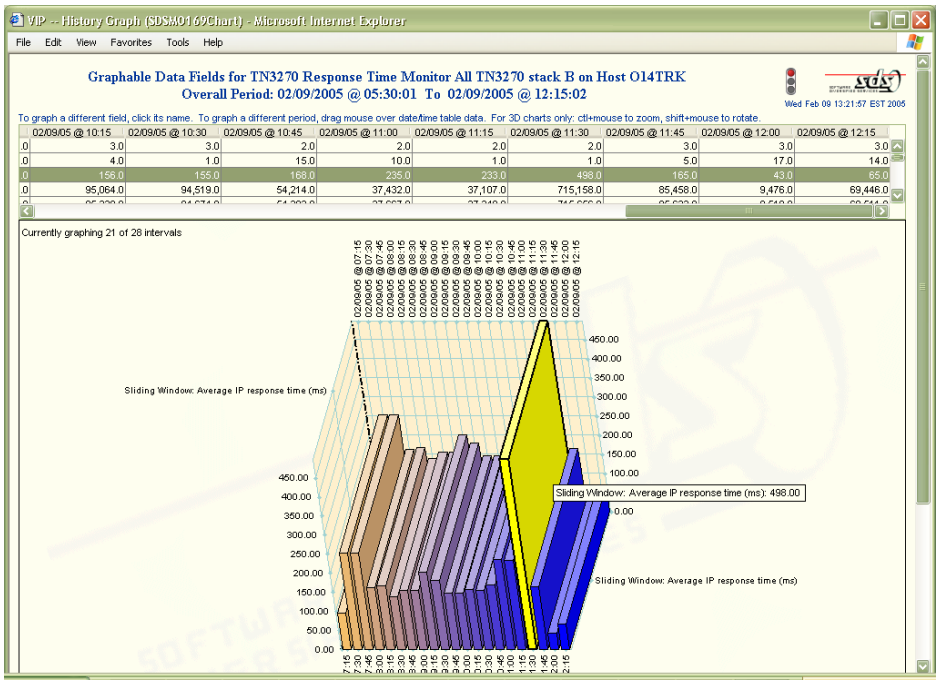


Developed for SDS:
by Anura Gurugé
April 2005

SOFTWARE DIVERSIFIED SERVICES

www.sdsusa.com

TABLE OF CONTENTS



Charted VIP v4 response time analysis data from the new RTM feature.

Mainframe TCP/IP Problem Resolution, in Real-Time, with SDS VIP v4

Software Diversified Services (SDS)

VitalSigns for IP

Proactive, anticipatory management

TCP/IP networks are now the primary mission-critical data backbones for today's mainframes. They have proved to be remarkably reliable and resilient even by the high-availability benchmarks associated with the SNA networks that they so summarily displaced. Mainframe TCP/IP networks, nonetheless, are deceptively complex and invariably convoluted, on both the network and mainframe sides.

Given this intrinsic complexity, there is much that can go wrong, very quickly and dramatically – and in reality, often does. Though these problems may not cause total network outages, they certainly disrupt application availability, response times, service-level expectations, transaction volumes and end-user productivity. Because these networks are truly mission-critical, there is always a tangible lost opportunity cost even with the smallest of glitches.

Hence, all mainframe shops need an incisive, proactive mainframe TCP/IP monitor that is able to continually keep tabs on the entire system, end-to-end, in real-time, to detect any and all problems – irrespective of how innocuous they first appear – before they become disastrous. *SDS' VIP is a proven, high-performance mainframe TCP/IP monitor that cogently addresses this need.* VIP is noted for not having any blind spots, whatsoever; for the breadth of its monitoring scope; for its agility; and for its innovative agent/server architecture that minimizes CPU utilization.

This white paper highlights **5** of the most common, high-profile, operations disrupting TCP/IP problem scenarios that currently occur in mainframe environments. It shows how VIP v4 can help you detect and resolve these problems, quickly and easily, before they snowball into service disrupting show-stoppers.

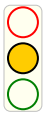
These 5 problem scenarios are:

1. Hung applications; i.e. applications that have failed in some way.
2. FTP problems, including failed FTP logins.

3. Inoperative remote devices and nodes, including routers, switches, firewalls, IP printers and Linux/AIX systems (including LPARs).
4. Unexpected, periodic spikes in TCP/IP resource utilization.
5. Degradation in response times.

Before describing in detail how these 5 TCP/IP problem scenarios can be detected and resolved using VIP v4 (starting on page 10), it is beneficial to briefly touch upon four topics that pertain to the methodology advocated in this white paper. They provide the pertinent context to the subsequent technical discussions, justify the use of certain techniques over other alternatives, and demonstrate how best to achieve genuine real-time system monitoring. These four topics, discussed starting on page 5, are:

- The inherent complexity of mainframe TCP/IP networks, particularly in comparison to SNA networks, and thus the need for an incisive TCP/IP monitor that can help system operators transcend the complexity and instead focus all of their efforts on successfully monitoring and managing the system.
- The inescapable advantages of using *multiple techniques*, in parallel, for obtaining requisite TCP/IP management data, rather than being tied to just one particular scheme (e.g. packet-tracing) – thus avoiding the dangers of blind-spots, expediting problem detection, minimizing mainframe resource consumption, and greatly increasing overall system efficiency.
- The agent/server architecture of VIP v4 that extends reach, expedites deployment, provides redundancy, and conserves mainframe CPU utilization.
- Basic, common features in VIP v4, such as the *at-a-glance* displays (page 5)and the red-amber-green alert status semaphore icon (right), that greatly simplify and facilitate overall, end-to-end system/network monitoring – in real-time.

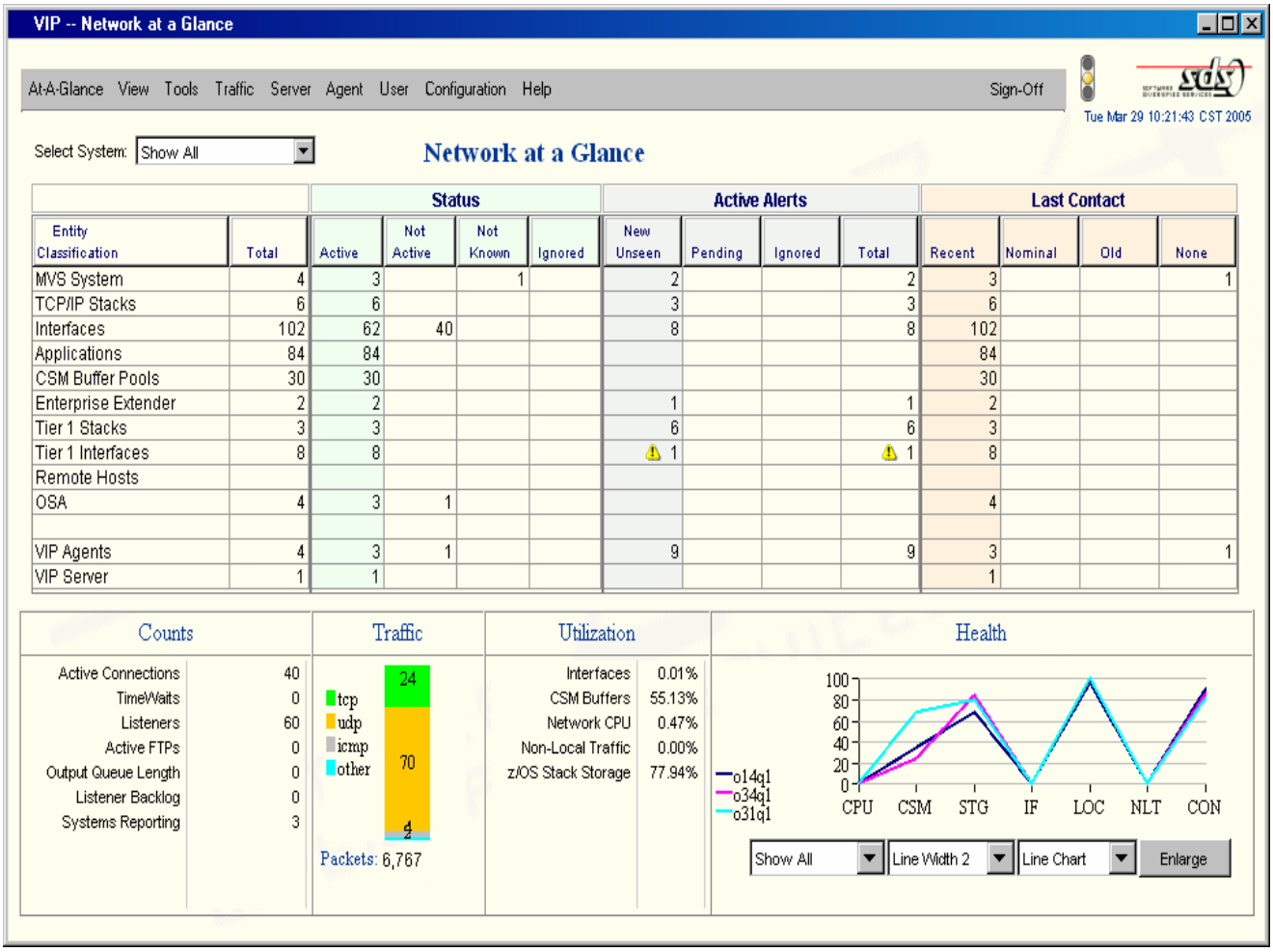


It is recommended that the companion white paper to this, entitled *Mainframe TCP/IP Management for Zero Downtime, High Performance Operations*, is used as an additional reference to augment the information presented here. This white paper is also available from SDS at www.sdsusa.com.

MAINFRAME TCP/IP MANAGEMENT

FOR ZERO DOWNTIME, HIGH PERFORMANCE OPERATIONS

SOFTWARE DIVERSIFIED SERVICES (SDS)



The information-packed (and highly popular) VIP v4 "Network at a Glance" screen provides real-time, consolidated status, activity and utilization data, spanning *multiple* 'MVS' systems on one easy to read screen - with all outstanding alerts clearly highlighted with color coded symbols.

INHERENT COMPLEXITY

In marked contrast to the homogeneity of SNA, TCP/IP networks are extremely multi-protocol. Different applications rely on different 'higher-level' protocols such as 'tn' (with or without SSL/TLS), HTTP(S), FTP, SMTP, OSPF, DNS etc., with these in turn running on top of either TCP, UDP (e.g. Enterprise Extender) or even ICMP (e.g. Ping). The problem scenarios discussed in this document reflect this multi-protocol aspect with one scenario dedicated entirely to FTP whereas the slow response time scenario relates to interactive tn3270 sessions.

The network infrastructure of mainframe TCP/IP networks, in addition, tends to consist of, at a minimum, a plethora of disparate switches, routers and firewalls, from multiple vendors. TCP/IP networks are also considerably more free-wheeling, with no central focal point of control (comparable to an SNA SSCP). Thus they tend to be much less deterministic. This can impact resilience as well as response times.

The mainframe side is also considerably more complex of late, with most machines now running multiple LPARs, possibly with multiple IP stacks per LPAR – with Linux LPARs gaining in popularity. IP-based HiperSockets, a cross-memory 'virtual LAN' mechanism that uses the new Queued Direct I/O (QDIO) protocol, has become the *de facto* means for all intra- and inter-LPAR communications. Furthermore, Virtual IP addressing (i.e. VIPA) with the option for dynamic VIPA takeovers across a sysplex has become the norm for mainframe IP networking. In parallel, with 37xx FEPs now discontinued, high-speed OSA and OSA-Express adapters, working at speeds up 1 gigabit per second, are becoming the accepted means for network attachment.

Given all of these factors, one should never underestimate the challenge of successfully, and proactively managing a large, high-volume, mission-critical mainframe TCP/IP network. The TCP/IP problem detection and resolution recommendations and techniques described in this white paper should be considered against this backdrop of overall complexity. You will then realize that the solutions being advocated here, in general, circumvent much of the TCP/IP intricacies, and enable system operators to focus on maintaining high-throughput, mission-critical operations without getting impeded by the complexity.

MULTIPLES SCHEMES TO EXTRACT MANAGEMENT DATA

When it comes to mainframe networks, SNMP, contrary to what some vendors purport, is *not the only*, and *certainly not the best*, means for obtaining incisive, real-time TCP/IP management data. SNMP is imperative for managing network devices [e.g. routers, firewalls] and remote hosts. However, in the case of 'MVS' mainframes relying on SNMP, without question, proves to be extremely inefficient, cumbersome and sluggish.

For a start, in order to use mainframe SNMP one has to configure and activate a *polling-driven*, OSNMP daemon for each IP stack that needs to be monitored. To obtain the necessary SNMP data, from the relevant MIB, the OSNMP daemon for each stack has to be repeatedly polled, via UDP packets. Often, these OSNMP polls result in large amounts of superfluous, redundant data (e.g. previously sent and since unchanged records such as the contents of routing tables) that unnecessarily wastes bandwidth and slows down data analysis.

The irony here is that all of the SNMP MIB data, for activity associated with any given IP stack, originates at that stack. In reality, each 'MVS' IP stack maintains an extensive array of management-specific data – with the z/OS IP stack, for example, containing 43 separate performance related statistics just for TCP/IP traffic! VIP obtains as much management data as possible directly from the IP stacks, using an efficient, IBM-provided API that works on a cross-memory basis between the stack and a mainframe-resident VIP agent.

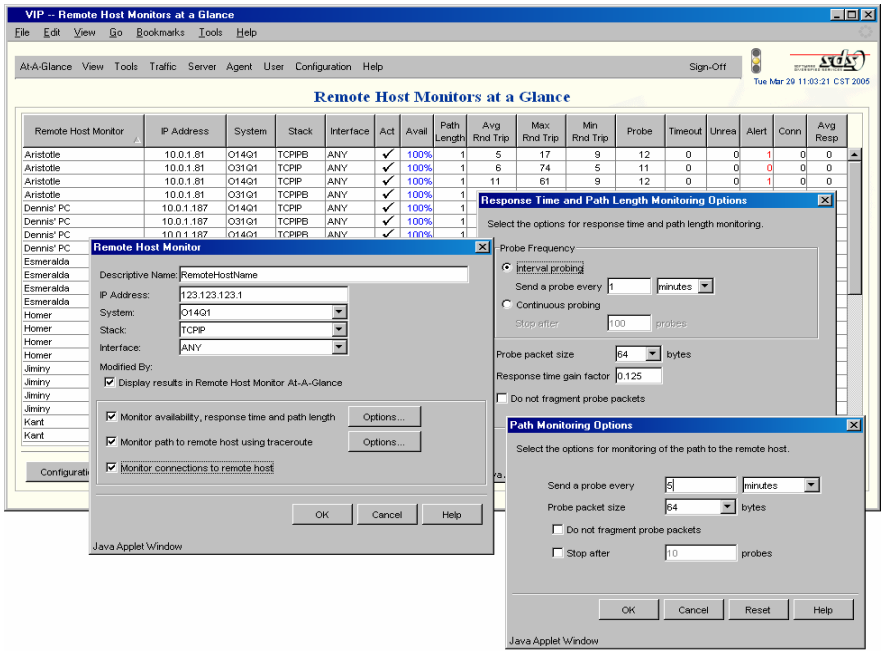
VIP's direct stack access scheme eliminates all of the overhead and inefficiency associated with the OSNMP daemon polling approach. Moreover, bandwidth and CPU cycles are not wasted transmitting unnecessary, 'throw-away' data. With direct stack access, VIP v4 can get exactly what it needs, when it needs it – on-demand. Hence all versions of VIP are noted for their parsimonious CPU usage along with ultra-fast, low-latency alert postings and data displays.

Relying predominantly on packet-tracing, as do some other mainframe monitors, is also not judicious. As with using OSNMP, relying heavily on packet-tracing is inefficient and carries a heavy overhead in terms of CPU cycles, memory usage and page swaps. Extensive packet-tracing, as is well known, slows down both network traffic and mainframe performance.

Packet-tracing, moreover, does not permit the detection of crucial events such as a burst of IDS activity denoting a potential security crisis, an increase in the connection backlog to an application indicating that the application may be in trouble, or packets being dropped because a remote system is not responding. Packet-tracing, as such, if used as the primary data extraction scheme, can result in extremely dangerous blind-spots.

Screen-scraping, another technique preferred by some other products, is now an outmoded legacy methodology, in that all of the data available with this approach can be obtained more quickly and with considerably less overhead using direct stack access.

The bottom line here is that an ideal mainframe TCP/IP monitor will not rely on just SNMP, packet-tracing or screen-scraping. Instead, it will obtain as much information as it can via direct stack access, and then complement and augment that data with additional information obtained using SNMP, packet-tracing, Ping and trace-route. *This is exactly what VIP v4 does*.



VIP, though relying on direct stack access for much of its management data, still includes comprehensive SNMP support for monitoring remote hosts. The Remote Host Monitors at a Glance display is shown here along with configuration panels.

Direct stack access is a well-established trademark of VIP. VIP, however, also includes uncompromised SNMP MIB Inquiry support that embraces 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). VIP v4, in addition, includes powerful packet-tracing functionality. VIP uses packet-tracing as an incisive diagnostic tool for problem isolation, as well as the basis for its tn3270 response time monitoring (RTM).

The VIP approach of judiciously using multiple data extraction schemes, *on-demand*, results in an unmistakable synergy. It gives you get the best of all worlds when it comes to comprehensive, real-time management visibility with minimal CPU overhead.

AGENT/SERVER ARCHITECTURE OF VIP

In addition to its partiality for direct stack access, another key differentiating characteristic of VIP is the flexible, caveat-free, agent/server architecture which has been a core design feature from the start. With this approach, SDS provides VIP monitoring agents written in optimized assembler for maximum speed and efficiency, for 'MVS' systems ranging from OS/390 v2.9 all the way through to z/OS v1.6.

The VIP servers are implemented in Java. As such, they can be deployed on PCs running Windows, on Linux/Unix servers (including Linux LPARs), or on a 'MVS' LPAR with Unix System Services (USS). *Management data gathered by the 'MVS' agents are fed, in real-time, to one or more VIP servers*. To eliminate unnecessary resource consumption, the VIP agents only transmit new data (i.e. data that has changed) to the servers. This keeps the agent-server traffic down to a minimum and ensures that management-related activity does not slow down the production workloads. The ability to easily deploy and use multiple VIP servers in parallel guarantees automatic resilience against potential server failures for *zero downtime* operations.

VIP's agent/server architecture, with its multi-server capability, offers numerous tangible advantages that have been repeatedly confirmed by existing VIP customers. Key among these being:

- Minimal utilization of mainframe CPU cycles.
- Unrestricted and readily extensible support for multi-LPAR, multi-mainframe networks with the ability to easily and non-disruptively add or eliminate LPARs or mainframes from the network.
- Ability to implement redundant, fault-tolerant configurations for *zero downtime* operations.

- Low total cost of ownership (TCO), given that the VIP servers can be readily implemented on economical, PC-based Windows or Linux servers.
- Ability to non-disruptively change or upgrade the platform on which a VIP server is deployed without impacting mainframe operations or interrupting overall management visibility of the network.
- *Offloading* of the network monitoring related data processing, data analysis and data presentation functions so that these functions do not impinge upon and negatively impact mainframe production workload processing.

SIMPLIFYING AND EXPEDITING MAINFRAME TCP/IP MANAGEMENT

The overarching design goal of VIP is that of simplifying the task of managing complex mainframe TCP/IP networks. VIP strives to be intuitive, cooperative and proactive. To this end, VIP includes a plethora of features that continually assist system operators to be more alert, responsive and productive. The simple but highly innovative red-amber-green alert status semaphore icon displayed on most VIP display screens is a good example of this. This unmistakable semaphore provides operators with an instantaneous health check of the network. A color change on this icon, particularly a change away from green or amber, will denote a change that one or more "attend" or severe level alerts need investigating.

Prompted by this heads-up, operators can then drill down deeper, using all of the various VIP tools, to quickly determine what has changed and what action they should take. The 9 incisive and highly informative, at-a-glance screens supported by VIP further facilitate rapid response on the part of the operators. The 9 'at a glance' displays supported by VIP v4, most of which can be individually customized to display data in a format best suited for a given installation, show:

1. Networks	2. Alerts	3. Application
4. System activity	5. FTP	6. Tn3270/telnet
7. OSA status	8. Remote host status	9. Enterprise Extender

The bottom line here is that VIP v4 is inordinately powerful, competent and efficient without, however, being complicated or unwieldy. *That truly sets it apart*. The 5 problem detection and resolution scenarios described in the remainder of this white paper will repeatedly demonstrate this underlying (and distinguishing) ease-of-use characteristic of VIP. Ease-of-use is such a basic tenant of VIP that it would be difficult, indeed, to find a problem scenario that would not end up underscoring this trait.

SCENARIO #1: HUNG APPLICATIONS

Hung applications result in major lost opportunity costs in mission-critical mainframe networks. Hung applications impact productivity, lead to lost transactions and infuriate users. A powerful mainframe IP monitor thus needs to provide operators with very straightforward means by which to quickly and easily detect applications that may be in a hung state. VIP v4, with its emphasis on extracting key management data directly from IP stacks, excels at providing very fast 'heads up' to operators about potentially hung applications. VIP v4 is also very good at highlighting applications under duress so that operators can intervene before the application crashes or starts rejecting transactions. Thus with VIP v4 operators can be ahead of the game when it comes to dealing with application failures. This minimizes lost opportunity costs and forestalls user complaints.

Early Warning, At a Glance, of Application Status

VIP v4's easy to follow **Applications at a Glance** display contains increased backlogs and connections drop counts. A sudden spike in these counts can indicate a hung application or an application in duress. Operators can also detect potential problems with applications by using the Activity at a Glance screen and selecting the *"summarized by system and application"* option. This will offer an invaluable and insightful view into application activity. With VIP v4 you can then drilldown on each application to obtain more data on activity and performance. The activity and performance metrics provide operators with comprehensive details that will help them to quickly determine if an application is hung, or is performing below performance expectations.

Select System: Show All

Applications at a Glance

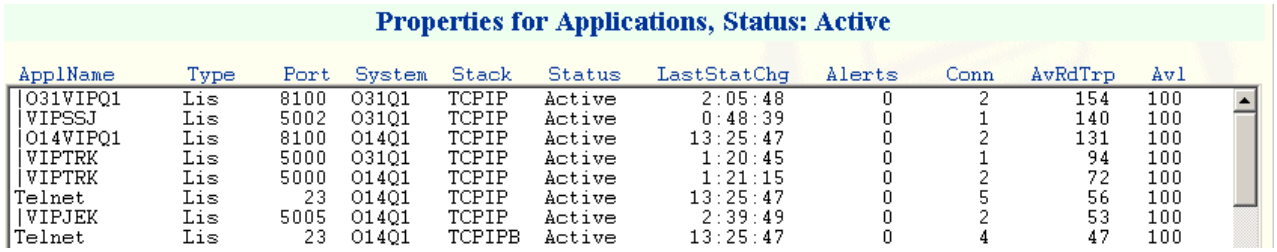
System	Application	TCP/IP Stack	Type	Listen Port #	Active	Total Conn	Avail %	Avg rTrip ms	Min rTrip ms	Max rTrip ms	Active Alerts	Accept Count	Curr Bcklg	Max Bcklg	Conn Drops	Prop	Hist	Tools
O14Q1	OSNMPDB/OSNMPDB	TCPIPB	L	1027	✓	0	100	0	0	0	0	0	0	5	0			
O31Q1	OSNMPDB/OSNMPDB	TCPIPB	L	1027	✓	0	100	0	0	0	0	0	0	5	0			
O14Q1	TCPIP/TCPIP	TCPIP	L	1025	✓	1	100	11	4	66	0	1	0	10	0			
O31Q1	TCPIP/TCPIP	TCPIP	L	1025	✓	1	100	13	7	75	0	1	0	10	0			
O14Q1	TCPIPB/TCPIPB	TCPIPB	L	1025	✓	1	100	5	3	27	0	1	0	10	0			
O31Q1	TCPIPB/TCPIPB	TCPIPB	L	1025	✓	1	100	16	6	51	0	1	0	10	0			
O14Q1	VIPDEV/VIPDEV	TCPIP	L	1029	✓	1	100	7	4	164	0	10	0	10	0			
O14Q1	VIPJEK/VIPJEK	TCPIP	L	5005	✓	2	100	85	6	167	0	2	0	10	0			
O14Q1	VIPJEK/VIPJEK	TCPIPB	L	5005	✓	0	100	0	0	0	0	0	0	10	0			
O14Q1	VIPSSJ/VIPSSJ	TCPIP	L	5002	✓	0	100	0	0	0	0	0	0	10	0			

VIP v4 Applications at a Glance display that contains backlogs and connections drop counts that provide operators with early warnings of potentially hung or poorly performing applications.

VIP v4 permits operators to request the automatic generation of an alert when a preset connection backlog threshold is reached. Operators are notified of such

alerts in the **Alerts at a Glance** display as well as by the VIP alert semaphore. Alert counts, per application, also appear in red in the Applications at Glance display. Operators can then check the Applications at a Glance or Activity at a Glance screens to determine which application or applications may not be responding or performing within expected limits. The operator can then select an application that appears to be hung (e.g. because of a spike in its backlog count) and then check for active alerts, connection drops, and round-trip times for this application.

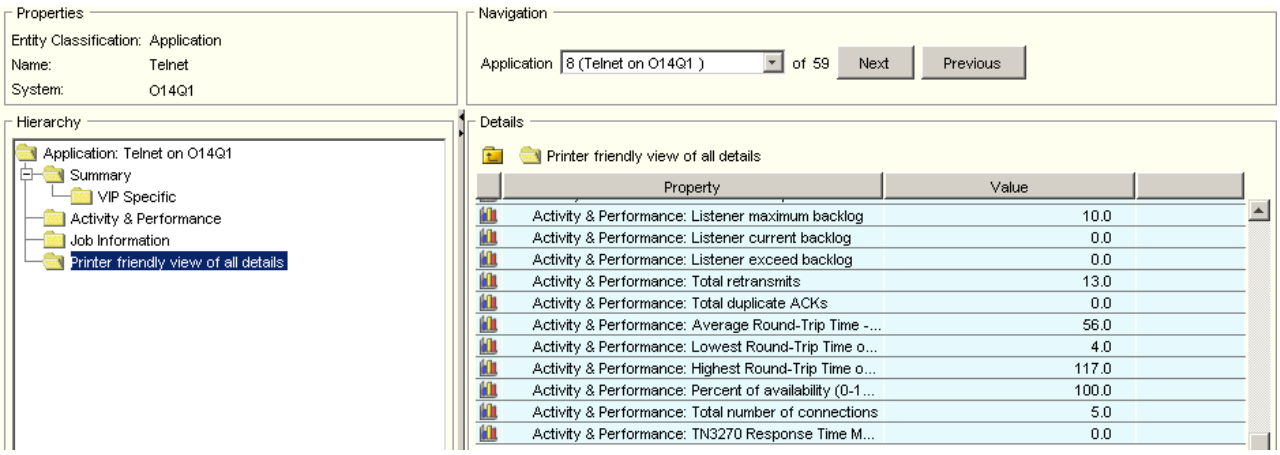
Selecting the properties view for a suspect application and then drilling down on the information available about that application will provide operators with a wealth of pertinent application specific details (as shown in the two screen shots below) that will help them determine the true status and health of that application.



Properties for Applications, Status: Active

ApplName	Type	Port	System	Stack	Status	LastStatChg	Alerts	Conn	AvRdTrp	Avl
|O31VIPQ1	Lis	8100	O31Q1	TCPIP	Active	2:05:48	0	2	154	100
|VIPSSJ	Lis	5002	O31Q1	TCPIP	Active	0:48:39	0	1	140	100
|O14VIPQ1	Lis	8100	O14Q1	TCPIP	Active	13:25:47	0	2	131	100
|VIPTRK	Lis	5000	O31Q1	TCPIP	Active	1:20:45	0	1	94	100
|VIPTRK	Lis	5000	O14Q1	TCPIP	Active	1:21:15	0	2	72	100
Telnet	Lis	23	O14Q1	TCPIP	Active	13:25:47	0	5	56	100
|VIPJEK	Lis	5005	O14Q1	TCPIP	Active	2:39:49	0	2	53	100
Telnet	Lis	23	O14Q1	TCPIPB	Active	13:25:47	0	4	47	100

VIP v4 properties display screen for active applications.



VIP v4 printer friendly views of the detailed activity and performance data available for a single, selected application.

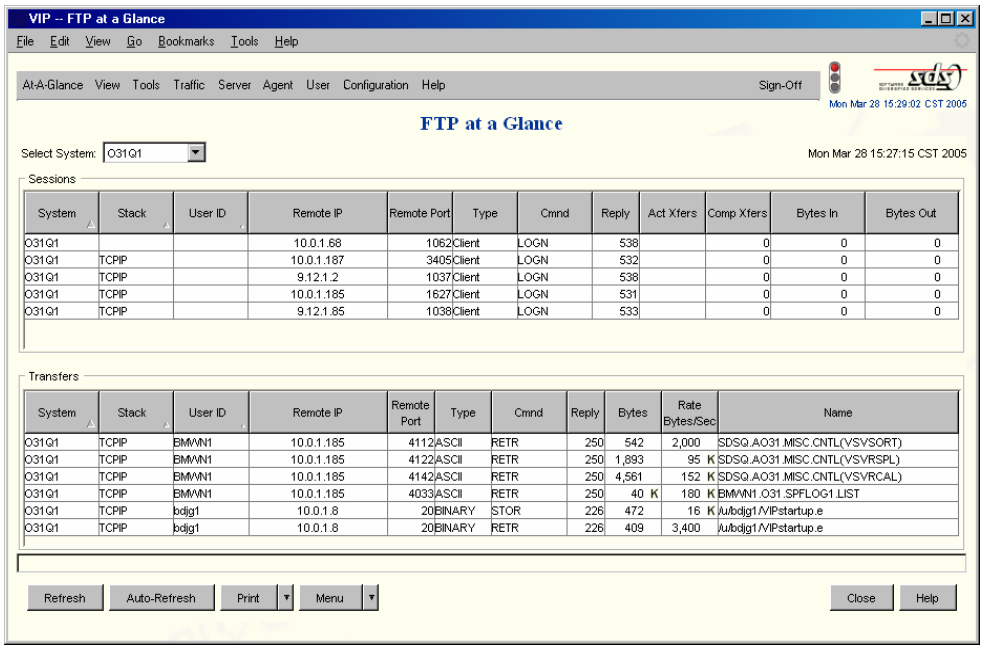
SCENARIO #2:
FTP PROBLEMS (INCLUDING FAILED LOGONS)

FTP-based file transfers invariably account for a very large portion of the mission-critical traffic on today's mainframe IP networks, especially with the growing importance of data transfer driven applications such as Web serving, corporate portals and data mining. Ensuring reliable, secure and efficient FTP transfers is thus an essential feature of current mainframe operations, with any FTP related anomalies likely to result in a flurry of urgent calls to the help desk.

To effectively track down and diagnose FTP problems operators need detailed information about both ongoing (i.e. currently active and recently completed) as well as past FTP operations. To be truly meaningful, this information cannot be restricted just to the FTP data sessions. It must include *control session* activity as well. An incisive real-time IP trace facility will also be required to troubleshoot complex FTP scenarios. In some instances it may be critical to have knowledge of unauthorized or excessive file transfers. To expedite problem detection and resolution all these FTP-related management functions need to be tightly integrated into a single intuitive, but comprehensive, management toolkit.

Automated Setup with VIP v4

VIP v4's highly proven FTP management feature, with its information-packed **FTP at a Glance** *and* **FTP History** *displays, satisfies all of the above criteria*. This logically designed capability automatically captures and consolidates all pertinent FTP related data including: user IDs, bytes transferred, throughput rates, datasets accessed, FTP return codes etc. Hence, with VIP v4 operators always have ready access to all the information they require, in clear and logical presentation form, to help them quickly identify and rectify FTP issues. VIP v4, with minimal FTP related set-up, thus accommodates all FTP file transfer scenarios and FTP monitoring requirements.



FTP at a Glance that provides details of recently completed FTP transfers including information about FTP logon failures. The information displayed includes: user IDs, IP addresses, port numbers, bytes transmitted, dataset names and return codes.

By default, data relating to problem-free FTP sessions and FTP transfer appear and stay on the FTP at a Glance display for two minutes after their close or completion. FTP logon failures will remain in the display for two hours. These FTP activity retention times can be customized, with VIP v4 supporting display periods up to 18 hours.

While FTP at a Glance deals with recent activity, a comprehensive log of all FTP activity that occurred during the last 3 months (or even more if so needed) is readily available via the VIP v4 FTP History display. In addition, VIP is able to deliver extensive batch reports on FTP activity covering: Activity Counts, Activity Data Set Summary, Login Failures, Summary by Host and User, Activity by User, and File Transfer Failures.

VIP v4 thus provides a wealth of FTP management data and tools, and moreover does so with minimal set-up requirements. VIP specific FTP related set-up, at most, is likely to just involve customizing the FTP activity retention period and adjusting the history storage allocation parameters to suit your exact needs. In order for VIP to automatically collect FTP information, the customer needs to have implemented and activated either the SMF 119 exit routine or the IBM NM API.

FTP Problem Detection Mechanisms with VIP v4

1. **FTP at a Glance**: This display, within a single window, provides a wealth of valuable information about current or recent FTP activity (as discussed above). VIP's FTP at a Glance provides a wealth of valuable information within a single window. Panels dealing with control and data sessions provide quick access to detailed information containing bytes transferred, throughput-rate, datasets accessed, commands performed, completed transfers per control session, and FTP return codes.

2. **Alerts & Alert semaphore:** VIP v4 *automatically* generates an alert whenever a FTP transfer ends up in a hung state. Operators are notified of such alerts in the **Alerts at a Glance** display as well as by the VIP alert semaphore. The Alerts at a Glance display shows alerts sorted by their ISO classification; e.g. security, performance, configuration and fault. Operators can click on an alarm to obtain additional details to help analyze the potential cause of an FTP hang.

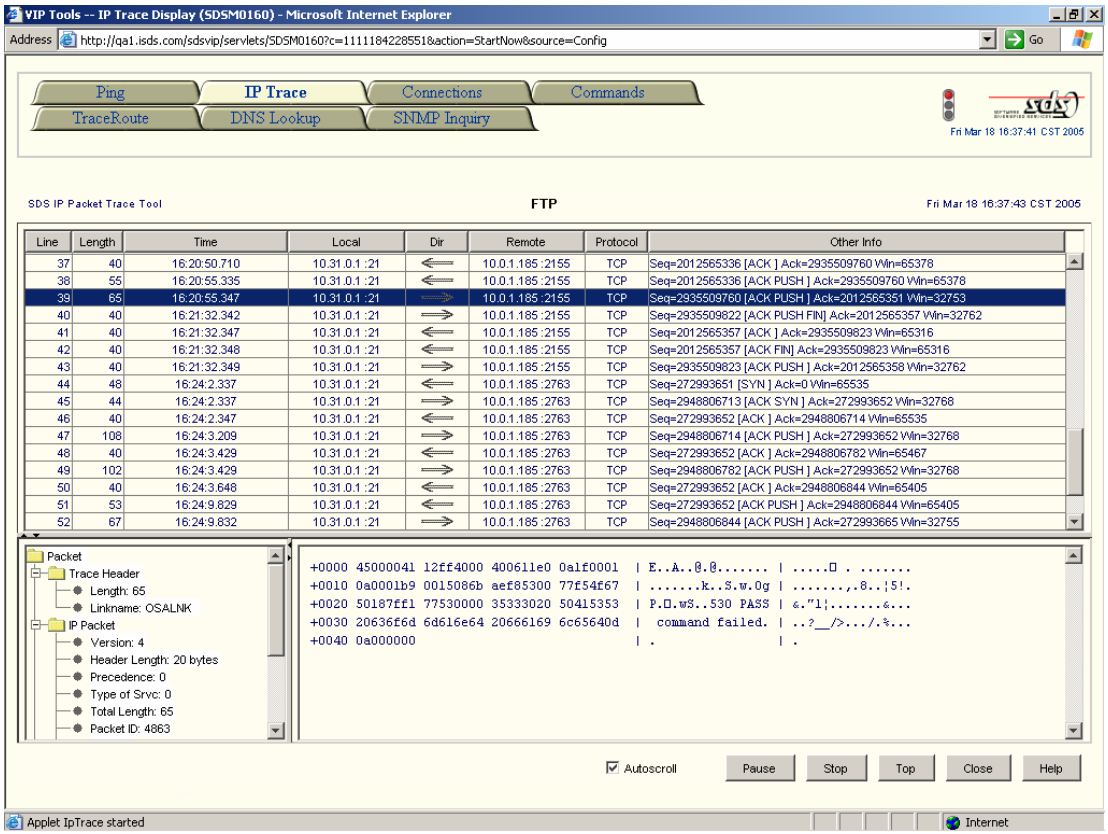
3. **Historic FTP Data:** If excessive or unauthorized FTP activity is suspected, operators can quickly and easily link to historical information directly from the FTP at a Glance screen to immediate track down past operations by the same user or users.

4. **FTP Return Codes:** With VIP v4 the original FTP return codes, for all operations, are displayed for both current and historic FTP activity. VIP v4

ensures that the full and exact range of FTP return codes are displayed with no omissions or modifications – including all of the various codes that specify exactly why an FTP logon was rejected. These FTP login failure related return codes indicate issues such as:

- Password is not valid
- Password has expired
- User ID has been revoked
- User ID is unknown
- User does not have server access
- User exit reject login
- Excessive bad passwords
- Group ID process failed

5. **Real-Time Packet Trace:** VIP v4, as discussed above, includes an incisive real-time IP trace facility. Thus with VIP v4 real-time IP packet traces can be invoked, at will, to obtain details of an entire FTP session, covering both the control and data sessions, bi-directionally. All that the operator has to do is to select the FTP protocol within the VIP v4 IP Trace display – as shown below.



VIP v4 IP Trace used to monitor the control and data flows of an FTP transfer.

5. **Batch Reports:** VIP v4, again as discussed above, can also generate batch reports that journal FTP activity. The FTP-related batch reports available with VIP v4 cover: Activity Counts, Summary of Data Set Access, Login Failures, Activity Summary Sorted by Host and User, Activity by User, and File Transfer Failures.

```
From:      2005-01-17 00:00:00                  SDS VIP Report Writer                                  Page:        1
To:        2005-01-23 24:00:00                      V3.5.0   087                                 Run Date: 01/21/05
Interval:  T                                                                                      Run Time:    10:30
Every:     30 Minutes                                                                               Report: FTPXFAIL
Shift:     1,2,3,4  Holidays:  *  Weekends:  *

                                    FTP Failed Transfers - Data Set Summary
                                                System O31Q1

                                                  Bytes    Bytes/  S Rply
       DataSet           Member    User     Date-Time     Xferred     Sec   C Code SEND STOR RETR APND DELT RENM OTHR
_____________________ ________ ________ _____________ __________ _______ _ ____ ____ ____ ____ ____ ____ ____ ____

SDSQ.ICAL5549.CICSDUMP           RFOG1    01/20/05 08:48  10,661,546 1193234 S  451    0    0    1    0    0    0    0
SDSQ.ICAL5549.CICSDUMP           RFOG1    01/20/05 09:08  62,029,948 1060287 S  451    0    0    1    0    0    0    0
                                                         ============================================================
SDSQ.ICAL5549.CICSDUMP           RFOG1                    72,691,494 2253521           0    0    2    0    0    0    0
                                                         ============================================================
               System:  O14Q1                             72,691,494 2253521           0    0    2    0    0    0    0

SDSQ.ICAL5544.CICSDUMP           YOBK1    01/21/05 18:06  12,750,595 1142526 S  451    0    0    1    0    0    0    0
                                                         ============================================================
SDSQ.ICAL5544.CICSDUMP           YOBK1                    12,750,595 1142526           0    0    1    0    0    0    0
                                                         ============================================================
               System:  O31Q1                             12,750,595 1142526           0    0    1    0    0    0    0




                                                         ============================================================
                  Grand Totals:                           85,442,089 3396047           0    0    3    0    0    0    0
```

Example of an VIP v4 batch report journaling failed FTP transfers summarized in terms of the mainframe datasets involved.

SCENARIO #3:
INOPERATIVE REMOTE DEVICES/NODES, INCLUDING ROUTERS, SWITCHES, FIREWALLS, IP PRINTERS AND LINUX/AIX SYSTEMS (INCLUDING LPARS)

In most mainframe IP networks, the mainframe, though pivotal, is still but the tip of the iceberg relative to the overall sprawl and complexity of the network. Many problems impacting mainframe operations are likely to be caused by entities external to the mainframe. To ensure that operators have a powerful **focal-point** for overall network control, VIP v4 is designed to be able to oversee remote devices that occur within the network. These could include SNMP capable devices such as router, switches, firewalls, Linux/Unix systems as well as non-SNMP capable devices such as IP Printers and desktops.

However, in many mainframe IP networks, the devices that are said to constitute the network fabric are typically managed, independent of the mainframe operations, by a specialized network managers using a SNMP-centric network management platform. Thus, VIP v4, as a mainframe IP monitor, may not have to keep tabs on all the devices in the network. Consequently, VIP v4 expects to be told of the external devices that its responsible for monitoring. This eliminates duplication and ensures that the appropriate *'spans-of-control'* are maintained between the mainframe and network operations groups.

The monitoring of all external devices are realized through VIP v4's sophisticated **Remote Host Monitoring (RHM)** tool. By default, RHM does not monitor any external devices to begin with. External devices that are to be monitored by VIP v4 thus need to be defined to RHM via an intuitive, Web browser-based graphical user interface. Since RHM can adroitly monitor both SNMP and non-SNMP entities VIP v4 can serve as a single, yet powerful and incisive window into the overall health of any IP network and forewarn operators of impending hot spots. With VIP v4 mainframe operators can once more act as the focal point for overall mainframe network management.

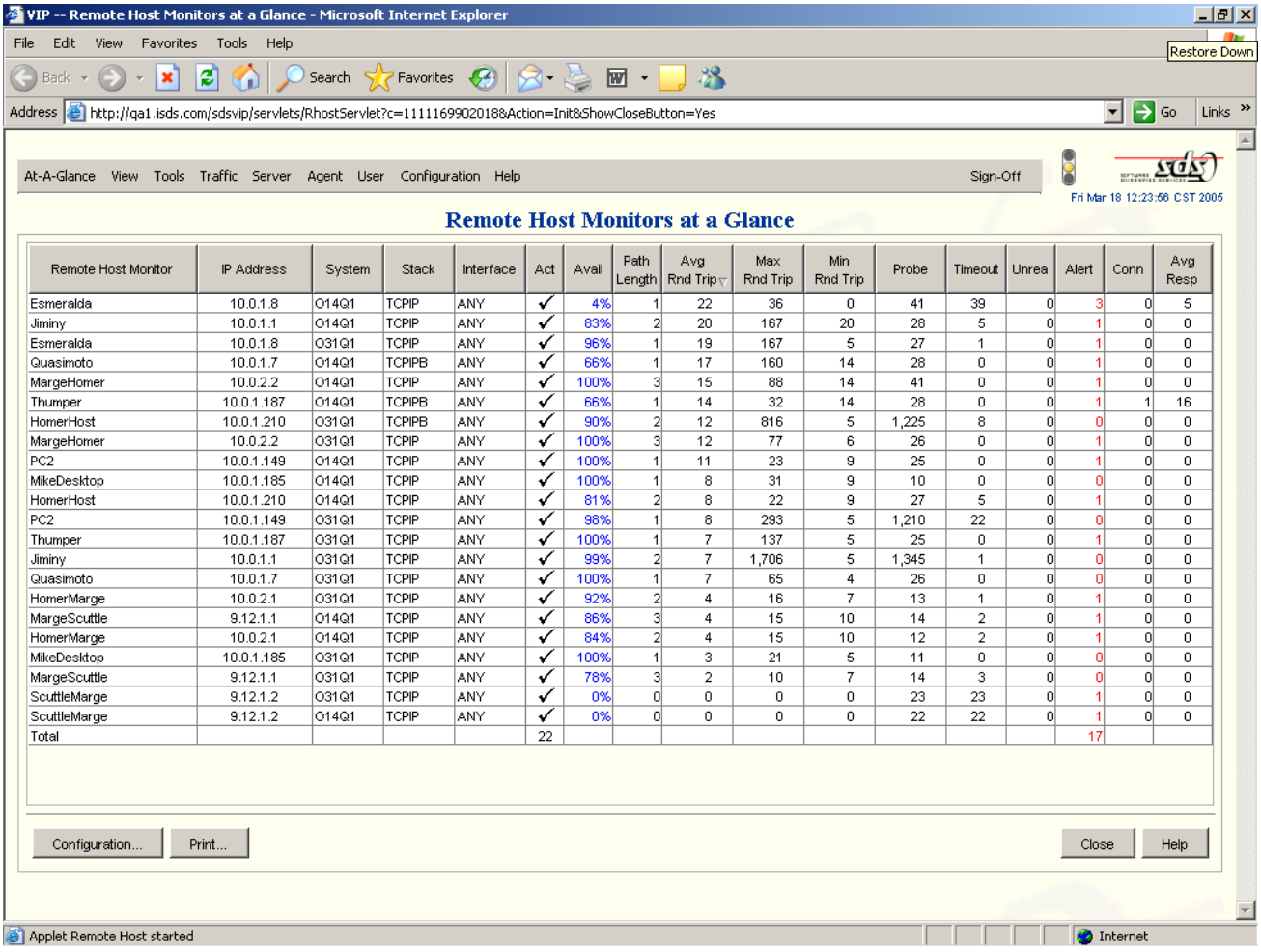
CONFIGURING RHM TO MONITOR EXTERNAL ENTITIES

1. Using RHM's Web browser-based GUI, define a descriptive name, IP address, system, stack, and interface for each external entity that needs to be monitored by VIP v4. Since VIP v4 is a mainframe-based monitor, operators can, where applicable, identify external entities using mainframe-oriented addresses. For example, if specifying a switch connected to an OSA interface to be managed, one could identify this switch in terms of its VIPA address, OSA address, or IP address. Thus VIP v4 gives operators the option of managing the network from a mainframe-centric standpoint or doing so independent of mainframe-centric addresses such as VIPA.

2. For each external entity to be managed by VIP v4, one can specify the exact parameters to be monitored by RHM, such as: device availability, response times, or path length.

3. One also can specify, for each entity, the exact frequency at which that entity should be monitored by RHM; e.g. at 5 minute intervals, at 1 hour intervals etc.

4. RHM also offers a very powerful and useful **stress testing** capability for determining the level of vulnerability of suspect external entities; e.g. a device suspected of dropping large quantities of packets during peak traffic loads. When invoked, this VIP v4 stress test tool can issue tens of thousands of probes, with elevated packet sizes, to the device in question – within a very short time period. Such stress tests can be used to quickly ascertain whether a remote device, e.g. a router, needs to be serviced, upgraded or replaced.



Remote Host Monitor	IP Address	System	Stack	Interface	Act	Avail	Path Length	Avg Rnd Trip	Max Rnd Trip	Min Rnd Trip	Probe	Timeout	Unrea	Alert	Conn	Avg Resp
Esmeralda	10.0.1.8	O14Q1	TCPIP	ANY	✓	4%	1	22	36	0	41	39	0	3	0	5
Jiminy	10.0.1.1	O14Q1	TCPIP	ANY	✓	83%	2	20	167	20	28	5	0	1	0	0
Esmeralda	10.0.1.8	O31Q1	TCPIP	ANY	✓	96%	1	19	167	5	27	1	0	1	0	0
Quasimoto	10.0.1.7	O14Q1	TCPIPB	ANY	✓	66%	1	17	160	14	28	0	0	1	0	0
MargeHomer	10.0.2.2	O14Q1	TCPIP	ANY	✓	100%	3	15	88	14	41	0	0	1	0	0
Thumper	10.0.1.187	O14Q1	TCPIPB	ANY	✓	66%	1	14	32	14	28	0	0	1	1	16
HomerHost	10.0.1.210	O31Q1	TCPIPB	ANY	✓	90%	2	12	816	5	1,225	8	0	0	0	0
MargeHomer	10.0.2.2	O31Q1	TCPIP	ANY	✓	100%	3	12	77	6	26	0	0	1	0	0
PC2	10.0.1.149	O14Q1	TCPIP	ANY	✓	100%	1	11	23	9	25	0	0	1	0	0
MikeDesktop	10.0.1.185	O14Q1	TCPIP	ANY	✓	100%	1	8	31	9	10	0	0	0	0	0
HomerHost	10.0.1.210	O14Q1	TCPIP	ANY	✓	81%	2	8	22	9	27	5	0	1	0	0
PC2	10.0.1.149	O31Q1	TCPIP	ANY	✓	98%	1	8	293	5	1,210	22	0	0	0	0
Thumper	10.0.1.187	O31Q1	TCPIP	ANY	✓	100%	1	7	137	5	25	0	0	1	0	0
Jiminy	10.0.1.1	O31Q1	TCPIP	ANY	✓	99%	2	7	1,706	5	1,345	1	0	0	0	0
Quasimoto	10.0.1.7	O31Q1	TCPIP	ANY	✓	100%	1	7	65	4	26	0	0	0	0	0
HomerMarge	10.0.2.1	O31Q1	TCPIP	ANY	✓	92%	2	4	16	7	13	1	0	1	0	0
MargeScuttle	9.12.1.1	O14Q1	TCPIP	ANY	✓	86%	3	4	15	10	14	2	0	1	0	0
HomerMarge	10.0.2.1	O14Q1	TCPIP	ANY	✓	84%	2	4	15	10	12	2	0	1	0	0
MikeDesktop	10.0.1.185	O31Q1	TCPIP	ANY	✓	100%	1	3	21	5	11	0	0	0	0	0
MargeScuttle	9.12.1.1	O31Q1	TCPIP	ANY	✓	78%	3	2	10	7	14	3	0	0	0	0
ScuttleMarge	9.12.1.2	O31Q1	TCPIP	ANY	✓	0%	0	0	0	0	23	23	0	1	0	0
ScuttleMarge	9.12.1.2	O14Q1	TCPIP	ANY	✓	0%	0	0	0	0	22	22	0	1	0	0
Total					22									17		

Remote Host Monitor at a Glance display that serves as the center piece of VIP v4's powerful and sophisticated Remote Host Monitor (RHM) capability for managing both SNMP capable and non-SNMP capable SNMP external entities such as routers, switches, firewalls, Unix/Linux systems, IP printers and desktops.

EXTERNAL DEVICE MONITORING MECHANISMS WITH VIP V4'S RHM

1. **Alerts & Alert semaphore:** VIP v4 RHM will automatically generate an alert whenever there is a relevant status change in any of the external entities being monitored; e.g. increase in path length beyond the preset threshold. As already discussed relative to the previous problem scenarios, operators can keep track of unseen alerts via either the omnipresent VIP alert semaphore or the RHM at a Glance display.

2. **Locate most serious problems:** Sorting the RHM at Glance display entries by *average roundtrip values*, in descending order (by host), immediately ranks the entries such as that the entities with the most serious problems are shown at the top.

3. **Emergence of trends:** Regular monitoring of remote entities via RHM, over time, will help operators detect certain trends in terms of problem occurrences that could indicate underlying problems within a specific region, datacenter, or even a server rack.

4. **Early warning of potential problems:** A sudden elevation in round-trip times is invariably a sign that something may have gone awry within the networks. Operators can check for such round trip time elevations by keeping an eye on the RHM at a Glance display.

SCENARIO #4: UNEXPECTED, PERIODIC SPIKES IN TCP/IP RESOURCE UTILIZATION

Occasional spikes in TCP/IP resource utilization, in general, are to be expected and are a part of the normal course of events during a work day. There is likely to be a spike in resource utilization in the mornings as users log into the system for the first time. There could also be a spike towards the end of the day when users upload files to the mainframe before logging off for the day. Operators are aware of such spikes and expect them to occur.

Unexpected spikes in TCP/IP resource utilization could, however, also indicate a denial of service attacks or hung applications. Thus it is prudent to monitor such spikes and investigate them. In some instances they may prove to be an early indication that certain components of the network (including the mainframe) may warrant an upgrade, or that resources may need to be reallocated to better balance network needs. Diligence in monitoring such spikes could also determine whether installations may be able to benefit from the capacity on demand options now available on new IBM mainframes.

A Two Step Process: Detection Followed by Investigation

Before one can investigate spikes in TCP/IP resource utilization, one needs to be able to detect that such a spike is occurring or has just occurred. VIP v4 permits quick and early detections of such spikes. Once you have established that a spike did occur then you need to determine the cause of that spike in terms of who, what, when and why. VIP v4 includes a well integrated set of interactive tools to help operators track down and investigate these spikes.

These VIP v4 capabilities include the Activity at a Glance, with its penetrating Heavy Hitters option, and the Connection Explorer displays. All of these VIP v4 displays, in addition, support extensive drilldown options to enable operators to obtain progressively more detailed information about a specific application, connection or resource.

To help narrow down possibilities, operators can also have VIP v4 summarize network activity by System and Stack. The results of this display can then be sorted by "share"; i.e. the percentage of activity attributed to a given stack. Using this information, coupled with what is available from the Heavy Hitters display (sorted by interface/connection), operators can quickly and decisively identify who or what caused a spike in TCP/IP resource usage.

Activity at a Glance

Activity summarized by: System and Stack

System	Stack Name	Sha-re	1 Min In Bytes	1 Min Out Bytes	5 Min In Bytes	5 Min Out Bytes	(Δ) In Packets	(Δ) Out Packets	(Δ) Loopback Packets	(Δ) In IF Discards	(Δ) Out IF Discards	(Δ) In IP Discards	(Δ) Out IP Discards	(Δ) Forward
O31Q1	TCPIP	47%	338,701	450,545	1,520,427	2,265,310	4,117	4,203	0	0	0	4,654	0	0
O14Q1	TCPIP	40%	162,359	517,597	978,619	3,693,178	2,655	3,552	0	1	0	2	0	0
O31Q1	TCPIPB	11%	118,394	74,823	378,173	198,149	244	189	824	4	0	255	0	0
O14Q1	TCPIPB	1%	4,555	14,205	18,806	91,026	15	15	0	0	0	0	0	0
	Total	100%	624,009	1,057,170	2,896,025	6,247,663	7,031	7,959	824	5	0	4,911	0	0

VIP v4's highly informative (and extremely popular) Activity at a Glance display.

Heavy Hitters

Wed Mar 23 12:21:45 CST 2005

System: O14Q1 Stack: TCPIP Heavy Hitters: Connection

Rank	Application Name	Local IP	Local port	Remote IP	Remote port	Conn ID	1 Min Total Bytes	1 Min In Bytes	1 Min Out Bytes	5 Min Total Bytes	5 Min In Bytes	5 Min Out Bytes
1	IO14VIPQ1	10.14.0.1	8100	10.1.31.1	1047	24CBFF	37,394	0	37,394	151,729	0	151,729
2	IO14VIPQ1	10.14.0.1	8100	10.0.1.68	2057	1EEC96	35,219	0	35,219	175,225	0	175,225
3	IO14VIPQ1	10.14.0.1	8100	10.0.1.103	1097	255F84	34,985	0	34,985	153,913	0	153,913
4	IO14VIPDM	10.14.0.1	8000	208.42.162.92	33933	23DE7A	30,738	0	30,738	132,191	0	132,191
5	VIPDEV	10.14.0.1	1423	10.0.1.74	34655	25529C	29,136	0	29,136	124,052	0	124,052
6	VIPTRK	10.14.0.1	5000	10.0.1.135	2677	244D1D	16,866	0	16,866	131,798	0	131,798
7	VIPTRK	10.14.0.1	5000	10.0.1.72	1704	241074	16,866	0	16,866	130,509	0	130,509
7	Total						201,204	0	201,204	999,417	0	999,417

The Heavy Hitters option within VIP v4's Activity at a Glance display.

OSA at a Glance

First Table: Physical Channels Second Table: LPAR Utilization

Physical Channel

OSA Name	Chp ID	Port Name	Index	Hdware Lvl	Chan Sub Type	Shr	Code Level	Status	Speed	1 Min Proc Util	1 Min PCI Bus	5 Min Proc Util	5 Min PCI Bus	1 Hour Proc Util	1 Hour PCI Bus	Avail	Alerts
OSA1	01	O31OSA1	1	Exp150	ETHR	Y	56A	Active	122 K	69%	35%	69%	49%	60%	42%	100%	0
OSA1	02	ifName string2	2	Exp150	ETHR	Y	56A	Active	94 K	69%	69%	69%	35%	69%	50%	100%	0
OSA1	03	ifName string3	3	Exp150	TR	Y	56A	Active	272 K	69%	55%	25%	61%	13%	19%	100%	0
OSA1	04	ifName string4	4	Exp150	ATM	Y	56A	Inactive	802 K	26%	41%	69%	66%	32%	69%	0%	1

LPAR Utilization

OSA Name	Chp ID	CSSID	LPAR Img	Port Name	Index	Status	1 Min Proc	1 Min KB In	1 Min KB Out	5 Min Proc	5 Min KB In	5 Min KB Out	1 Hour Proc	1 Hour KB In	1 Hour KB Out	Avail	Alerts
OSA1	01	0	0	O31OSA1	1	Active	69%	1,248 M	1,002 M	69%	3,165 M	3,171 M	69%	3,994 M	4,067 M	100%	0
OSA1	02	0	0	ifName string2	2	Active	57%	936 M	929 M	23%	3,076 M	3,078 M	67%	3,148 M	3,196 M	100%	0
OSA1	03	0	0	ifName string3	3	Active	69%	932 M	930 M	69%	3,081 M	3,082 M	69%	3,157 M	3,272 M	100%	0
OSA1	04	0	0	ifName string4	4	Inactive	4%	939 M	919 M	26%	3,093 M	3,080 M	62%	3,175 M	3,170 M	0%	0

Use VIP v4's OSA at a Glance to investigate a specific connection, in this instance an OSA connection, if unexpectedly heavy activity is shown for that connection in the Heavy Hitter display.

SCENARIO #5: DEGRADATION IN RESPONSE TIME

Response times tends to be the pulse of a mainframe network. They serve as a critical and infallible metric of overall network performance and health. One, however, needs to establish parameters for what is deemed to be the acceptable response time metrics for a given network, since the expectations for what is acceptable when it comes to response times can be somewhat nebulous, subjective and variable. Furthermore, the tolerance for degradation (or inconsistencies) in response times, however minute, also vary from user to user – and by application to application.

In a mainframe IP network, response time degradation may be caused by a multitude of possibilities. Some of the more common culprits are likely to include: excessive packet fragmentation (i.e. MTU size is too small); re-routing of packets over non-optimal links; excessive drain of CPU resources by an unrelated application or process, or even Path MTU Discovery (PMTUD) failures where fragmentation required ICMP messages are being blocked by a firewall or an incorrectly configured access list.

Multiple Response Time Troubleshooting Option with VIP v4

Troubleshooting response time degradation will likely involve investigating basic network connectivity as well as analyzing summarized activity of your systems, stacks, and applications. This can be achieved via methodical and judicious use of VIP v4 at-a-glance utilities – many of which have by now been discussed relative to the previous problem resolution scenarios.

Basic connectivity tests available with VIP v4 include VIP's Ping and Traceroute tools. In addition, operators can invoke VIP's IP packet trace to verify proper handling of fragmentation request responses. This can also help identify problems such as "Black Hole" where PMTUD fails because the necessary ICMP messages are not being received by the originating host, or "Stretch Ack" situations where a non-PMTUD TCP stack communicates with a PMTUD stack generating an ACK for every other full-sized segment. This latter scenario results in a PMTU that is a fraction of the advertised MSS with infrequent ACKs being generated.

VIP's Activity and Applications at a Glance displays, with the Heavy Hitters option (as previously discussed), can be used, very effectively, to determine there is abnormally high activity indicated for a particular stack or application. Operators can also determine if a particular set of users are consuming excessive resources.

In addition, VIP's Remote Host Monitor (RMH) can be configured to monitor availability, response time, and path length as discussed in scenario # 4 above. RHM will also automatically generate an alert if and when there is a path change, thus giving operators a heads up of potential changes in response time characteristics.

VIP v4's tn3270 Response Time Monitor (RTM) includes multiple threshold settings for in-depth and incisive response time monitoring. Alerts are automatically generated whenever any one of these thresholds is reached. It is possible to set these thresholds on a 'cumulative' basis for generating RTM alerts – as well as to specify an acceptable "overall average" response time setting.

Thus, with VIP v4, it is possible to specify that an alarm should be raised if less than 80% of transactions (over a pre-specified period of time) occur within 1 second, or more than 5% of transactions are taking longer than 10 seconds, or the overall average exceeds its threshold. It is possible to activate multiple VIP RTM monitors which in turn can concurrently track overlapping entities; e.g. a complete tn3270 server, a sub network and an individual link within that sub network. Individual RTM monitors can be activated on demand, or be set-up to be active per a predefined schedule, which can be specified in terms of a day, a date, a time of day etc.

Local	Dir	Remote	Protocol	Other Info
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155143033 [ACK] Ack=1318290660 Win=32632
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155144293 [ACK] Ack=1318290660 Win=32632
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155145553 [ACK PUSH] Ack=1318290660 Win=32632
10.31.50.5	⟸	10.99.44.1	ICMP	ABBR type=[Dest. Unreachable] code=[Frag. needed and DF set]
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155143033 [ACK PUSH] Ack=1318290660 Win=32632
10.31.50.5	⟸	10.99.44.1	ICMP	ABBR type=[Dest. Unreachable] code=[Frag. needed and DF set]
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155143033 [ACK PUSH] Ack=1318290660 Win=32632
10.31.50.5	⟸	10.99.44.1	ICMP	type=[Dest. Unreachable] code=[Frag. needed and DF set]
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155143033 [ACK PUSH] Ack=1318290660 Win=32632
10.31.50.5	⟸	10.99.44.1	ICMP	type=[Dest. Unreachable] code=[Frag. needed and DF set]
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155143033 [ACK PUSH] Ack=1318290660 Win=32632
10.31.50.5 :23	⟸	10.99.44.1 :17155	TCP	Seq=1318290660 [ACK] Ack=155143033 Win=65399
10.31.50.5 :23	⟸	10.99.44.1 :17155	TCP	Seq=1318290660 [ACK] Ack=155144143 Win=64289
10.31.50.5 :23	⟹	10.99.44.1 :17155	TCP	ABBR Seq=155144143 [ACK] Ack=1318290660 Win=32632

```
+0000 45c00240 a23f0000 fd01a635 0a632c01  | E..@.?.....5.c,. | ... s.....w.....
+0010 0a1f3205 0304f589 000004b0 45000514  | ..2.........E... | ......5i........
+0020 52834000 3d0673d9 0a1f3205 0a632c01  | R.@.=.s...2..c,. | .c ...cR........
```

VIP v4's powerful IP trace being used to track down the cause for a degradation in response times.

TN3270 Response Time Analysis

Wed Mar 23 10:11:45 CST 2005

Monitor	System	Status	Monitored Conns	Alerts	Sliding Total Trans	Sliding Avg IP	Sliding Avg SNA	Sliding Avg Total	L-O-M Total Trans	L-O-M Avg IP	L-O-M Avg SNA	L-O-M Avg Total	Resp within Bnd 1	Resp within Bnd 2	Resp within Bnd 3	Resp within Bnd 4	Resp over Bnd 4
o14djm	O14Q1	Active	6	1	98	29	14	43	130	31	12	43	99%	0%	1%	0%	0%
o14b	O14Q1	Active	5	0	14	17	51	68	214	18	51	69	92%	7%	1%	0%	0%
Bmwn	O31Q1	Active	2	2	100	34	22	56	609	21	28	49	66%	30%	1%	1%	2%
o31djm	O31Q1	Inactive	0	0	0	0	0	0	116	2	12	14	98%	2%	0%	0%	0%
o31sched	O31Q1	Active	0	0	0	197	42	239	20	198	43	241	100%	0%	0%	0%	0%
Total		5	13	3	212	277	129	406	1089	270	146	416	79%	118%	1%	1%	1%

VIP v4's tn3270(E) response time analysis option within the RTM feature.

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
IDS	Intrusion Detection System as now available within z/OS
MIB	management information base, a database of network management objects for a given entity
OSNMP	IBM provided daemon for using SNMP with 'MVS'
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