

March 2001

## Performance Monitoring of Heterogeneous Network Protocols in a Mainframe Environment

### VitalSigns for VTAM (VSV)

"A network monitoring system that only provides data on SNA or TCP is no longer acceptable. Today's large scale enterprises have a mixture of protocols, and the ability to monitor the enterprise, to baseline the information, and to study the data is of utmost importance to all IS management. Failure to monitor and proactively manage the network will result in the network managing the IS staff, rather than the IS staff managing the network."

John Lampi, CEO, Software Diversified Services

### The March and Development of Mainframe Communications Protocols

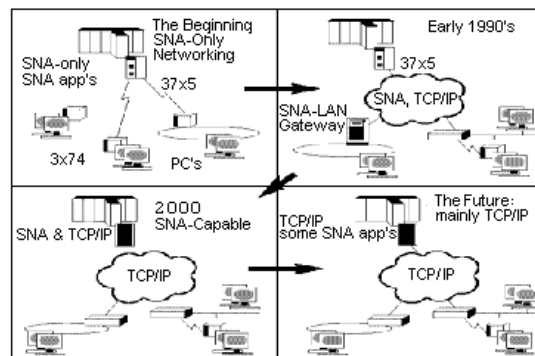
SNA, the backbone of enterprise networking, has had a remarkable history. Any business in the last quarter-century that has based its IS department around an IBM mainframe has been the recipient of the remarkable strength of the SNA protocol. However, as we begin the 21st century, the dominance of SNA is shared with TCP/IP implementations.

To be sure, enterprises that have mission-critical SNA applications will continue to use the protocol into the foreseeable future. However, the march toward an integration of the TCP/IP protocol into the networking framework of all IS departments is inescapable.

IS departments are migrating to integrated systems not because of any desire to be on the leading or "bleeding" edge of technology but rather because it is simply the direction that business has been headed. Companies that combine both mainframe technologies and Web-enablement, whether for Internet or Intranet functionality, invariably must have a heterogeneous network. The objective of the integration is greater accessibility, greater flexibility, reduced infrastructure costs, and integration of heterogeneous distributed systems.

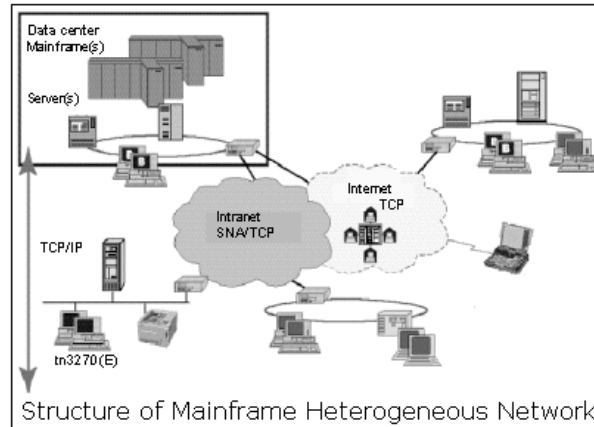
IBM estimates that in the year 2001, approximately 90% of all mainframe systems operating z/OS - OS/390 - MVS have TCP/IP installed. The incredible surge over the last five years of installations with TCP/IP and the continuation of the trend can be attributed to a concurrent surge in Internet/Web activity and IBM's strategic replacement of MVS. IBM's large-scale operating system replacements, OS/390 and z/OS, includes TCP/IP as part of the standard function. The reasons this upward trend has not been even more dramatic are that 1) it has taken IBM and Interlink Computer Services a period of time to create a TCP/IP software package that is at least as efficient as some seamless gateway alternatives and 2) IS departments have been cautious about making wholesale operating system changes. Post-Y2K growth in operating system changes and inclusion of TCP/IP is explosive.

Measurement of the reliability of SNA networks and end-to-end response time for these networks have been critically important to management. Often, on-time delivery and up-time of a network have been more important than the actual data delivered as a basis for confidence in an IS department. Conversely, if response time is slow and IS management is not able to maintain an extremely high level of network up-time, even the best data that is delivered can be called into question. Introduction of the TCP/IP component and the potential of utilizing this protocol to deliver more mission critical real-time information demands that monitoring of the overall network be considered a priority in any enterprise.



Standard or traditional IBM mainframe network monitoring systems have not, in the past, been able to meet the demands to allow IS management to adequately and proactively monitor the heterogeneous network. Most monitoring tools were lacking in either the breadth of protocols monitored or in the statistical warehousing of the data. Some network management systems, while having the ability to "see" the entire network, component by component, only alert you to the fact that a component has been "dropped." These may not notify you of trends that could have provided advanced warning of a potential critical situation. These monitors force the network staff into being reactive rather than proactive. Other monitors may adequately handle the mainframe SNA data, but another system is required to monitor the TCP/IP activity. Management of both or either component can be excellent, but if handled by different personnel within the enterprise it becomes necessary for senior personnel to coordinate and combine the information to obtain a total picture. This latter function is time and schedule dependent, making it possible to have "done everything right" but not being able to be proactive in your management, simply because all of the correct data arrived too late.

Software Diversified Services (SDS) is of the opinion that it has developed and enhanced an already highly successful software monitoring tool that now allows for heterogeneous network monitoring of SNA, its components, and TCP/IP. Built around SDS's VitalSigns for VTAM (VSV) software, the addition of TCP/IP monitoring now allows IS management to have a complete network picture in real time, with a historical repository of collected data and a flexible report writer that allows management to be proactive in the administration of the heterogeneous network of the 21st century.



## VitalSigns for VTAM development

VitalSigns for VTAM (VSV) has mirrored the direction and development of networks. Originally developed as a VTAM-only monitor by BlueLine Software, Inc., VSV proved to be an extremely reliable software tool with which IS departments could measure SNA network performance.

Based on the premise that the most reliable monitoring system is one that shows changes from one time period to another, VSV was developed with an integrated historical repository that holds all of the measured statistical data. VSV allows IS management to review and adjust baseline information on a continuous basis. The ability to have a baseline against which to start a measurement allows two very distinct advantages for any proactive management group.

\* Management and operators can quickly see trends as there are shifts from the baseline. Without the ability to note changes from a known starting point, management is unable to forecast required adjustments in order to keep the network operating at optimal capacity. Peaks and valleys of response time noted only on a short-term basis force management to react to a given situation without the ability to determine the potential long-term impact of the decision.

\* When given the ability to adjust baseline information, management provides itself with the security of knowing the resource adjustments they have taken, such as adding equipment, increasing bandwidth, or adding high-network-usage software, can be accounted for when they determine there are shifts in trends. This allows management to insure the changes they have undertaken were either entirely correct or in need of some further adjustment to insure the integrity of the system.

## How VitalSigns for VTAM (VSV) Works

VSV provides compressive monitoring of the network including VTAM and TCP/IP traffic, response time, and memory use for lines, controllers, applications terminals, LANS and gateways.

VSV works by a host-and-agent strategy. VSV Online resides on your host system and provides menu-navigated controls for data collection, storage, and reporting. Individual VSV agents collect data from NCP, VTAM, and TCP/IP facilities.

The TCP/IP agent resides on the IP host, where it communicates between VSV Online and the host's TCP/IP stack. It collects data about TCP/IP activity from the host's SNMP (simple network management protocol) daemon.

The TCP/IP agent also reaches out to gather data from any other IP host on the network, provided that host includes an SNMP daemon. All the agent needs is the IP address of the host and the security authorization for the daemon.

Host-and-agent technology provides critical advantages over other software alternatives. Primarily this methodology reduces the cycle usage and overhead associated with the monitoring process. It is extremely important that a monitoring system does not use so much of the system and network that it becomes part of any system resource problem. Additionally, host-and-agent software means that in a large-scale enterprise with multiple mainframes and with cross-domain communications, VSV only needs to be installed at a single location. This allows management to easily generate data on the overall network and to also break the data down by individual components of the network, therefore allowing for better and more timely allocation of resources.

## Collecting Performance Data

VSV uses four agents to collect performance data, one each for NCP, VTAM, SNMP, and a new MVS agent to collect and deliver better FTP statistics.

Complex networks with multiple CPUs, operating systems, domains, and NCPs can be monitored by a single installation of VSV communicating with multiple agents throughout the system.

VSV Online provides menu-navigated control over data collection, retrieval, and reporting. Current performance is reported online in a hierarchy of summary and detail displays. Long-term data can be reported to the historical file and displayed online or put into reports by the report writer utility included with VSV. Users may customize alerts regarding exceptional conditions for their particular environments. VSV Online also provides a tool for testing 3270 terminals to insure data delivery.

VSV Online is navigated through a hierarchy of menus, by a pop-up index of available displays, or with two- to eight-character "fastpath" commands to be typed at the command line of any display. The hierarchy of displays ranges from broad summaries to details about single lines or terminals. Navigate by selecting records, then selecting from a menu of the available details.

You can open, move, and control the size of any number of displays. The pop-up index can be made to list all the VSV displays, or just those you currently have open.

**Monitor Controls:** Performance monitoring is controlled by a menu-guided process of defining IP hosts, NCPs, VTAM applications, and terminals; selecting specific resources to monitor; specifying threshold values; and scheduling data retrieval. Monitoring can be set to begin automatically at system

startup.

**Data Retrieval:** VSV Online retrieves data from multiple agents and writes it to a single DASD repository. The data is first written to a collection file. When the file is full, VSV starts another one, for up to five files. At specified intervals, the data moves from the collection files to a recall file. The recall file can be displayed online and archived to tape.

**Reports:** VSV reports performance statistics by processing the data it has stored on DASD. It can recall immediate history--lag time is as short as one minute--for online display. It can report long-term data using batch processes and the Performance DataBase (PDB) Reporting Facility. VSV Online can write to SMF Type 28 records for processing by report writers that require that format--e.g. BGS's BEST/NET SNA and Merrill Consulting's MXG. It writes such data to sequential data sets or to z/OS SMF data sets.

**IP Ping Test:** VSV provides its own ping test to troubleshoot and verify connections between z/OS IP hosts.

**Exception Alerts:** VitalSigns can alert you about exceptional conditions--an NCP line operating at 60% of capacity, for example. At the control display, select records and fields to be monitored, specify thresholds, and specify routing for the alerts. Thresholds can be set at two levels for a given item: warning and critical. The Exception Summary Display reports all exceptions during the most recent monitoring interval and links to details about individual exceptions. Most other displays also include links to exception details.

Exception alerts can be sent to:

- \* The VSV log
- \* The system console
- \* NetView®
- \* NetMaster

## TCP/IP Data is Collected via Standard Network Systems

The data objects held by an SNMP daemon are defined by the "Management Information Base" (MIB), part of the worldwide design standards for TCP/IP networks. Among the SNMP data that VSV for TCP/IP collects are the following:

**Interface Configurations:** Given an IP address and password for a remote host, VSV for TCP/IP will learn that host's connection configuration, i.e. the number and type of I/O interfaces (token ring, Ethernet, frame relay, etc.) in the host's TCP/IP stack. VSV for TCP/IP will itemize the input and output paths for the stack, report the operational status of each interface, and provide counts of input, output, errors, and discards.

**Transport Services:** A daemon's UDP data describes datagram traffic, the bulk of the traffic on the Internet. Its TCP data describes traffic on "stream sockets," high-overhead connections for guaranteed delivery of accurate data--for file transfers, for example. For both UDP and TCP data, VSV reports numbers of packets and octets in and out, as well as errors and packets with unknown protocols.

**Network Services:** The network services layer of a TCP/IP stack provides IP services--meaning it accepts data for delivery or forwards it to another node in the network. Those tasks include fragmenting and reassembling packets. Network services also include handling ICMP commands--traffic between TCP/IP stacks that allows them to work cooperatively. Such commands include ping, echo, and DNS inquiries, for example. For both IP and ICMP, and for both input and output, VSV reports the numbers of packets delivered, forwarded, assembled, fragmented, and discarded; numbers of errors; numbers of octets per packet; and the maximum size of packets.

**System Services:** System services data describes the identity and configuration of a host and the activity of the SNMP daemon itself. This data is relatively static and does not measure performance, so VSV does not routinely collect it. VSV does, however, allow users to interactively query this data.

**z/OS-Specific Data:** IBM has extended the MIB in order to improve TCP/IP management on z/OS systems. VSV provides access to this z/OS-specific data.

**Telnet Statistics:** Telnet statistics report specific activity usually generated through port 23.

**FTP Statistics:** FTP activity is usually generated through ports 20 and 21. VSV reports names of files transferred, their origination and destination, their size, and who sent them.

**Socket-Level Statistics:** Measuring throughput is often not enough. VSV tells network service administrators who is using bandwidth, when, and why.

## Additional Features of VSV

- \* Online help for all displays, fields, and messages
- \* Automatic refresh of displays at regular intervals
- \* Security controls, mouse support, and tools for sorting, searching, filtering, and color-coding data
- \* Compliance with IBM's Common User Access/Systems Application Architecture (CUA/SAA)
- \* An interface for issuing VTAM display and vary commands
- \* Automatic updates of NCP definitions

## TCP/IP, VTAM, NCP, and RTM Methods and Information Gathered

### TCP/IP-Specific Information Harvested:

IP Data:

- \* Forwarding gateway (yes/no)
- \* Datagrams delivered
- \* Datagrams forwarded
- \* Default time-to-live for datagrams
- \* Datagrams discarded due to error
- \* Datagrams with invalid address
- \* Datagrams with unknown protocol
- \* Datagrams discarded for lack of route to destination
- \* Datagrams discarded for other reasons
- \* Maximum time fragments are held awaiting reassembly, in seconds

- \* Fragments needing reassembly
- \* Datagrams reassembled
- \* Reassembly failures
- \* Datagrams discarded because they could not be fragmented
- \* Fragments generated
- \* Routing entries discarded

#### TCP Data:

- \* Name of the algorithm that sets timeout value for retransmitting unacknowledged octets
- \* Minimum retransmission timeout permitted, milliseconds
- \* Maximum retransmission timeout permitted, milliseconds
- \* Maximum number of TCP connections supported
- \* Transitions to SYN-SENT from CLOSED
- \* Transitions to SYN-RCVD from LISTEN
- \* Transitions to CLOSED from SYN-SENT or SYN-RCVD and to LISTEN from SYN-RCVD
- \* Transitions to CLOSED from ESTABLISHED or CLOSE-WAIT
- \* Connections currently in ESTABLISHED or CLOSE-WAIT status
- \* Segments received
- \* Segments sent
- \* Segments retransmitted

#### Interface Data:

- \* Number of interfaces on the system
- \* I.D. number for each interface
- \* Manufacturer, product, version
- \* Type of interface
- \* Size, in octets, of largest datagram interface can transmit
- \* Current bandwidth, in bits/second
- \* Address of interface
- \* Desired status (up, down, testing)
- \* Current status (up, down, testing)
- \* Octets (or bytes) received
- \* Unicast packets delivered
- \* Broadcast or multicast packets delivered
- \* Inbound packets discarded
- \* Packets undeliverable due to errors
- \* Packets with unknown protocol
- \* Octets (or bytes) transmitted
- \* Packets seeking transmission to unicast address
- \* Packets seeking transmission to broadcast or multicast addresses
- \* Outbound packets discarded
- \* Outbound packets not transmitted due to error

#### UDP Data:

- \* Datagrams delivered
- \* Datagrams sent
- \* Datagrams received for which there was no application
- \* Datagrams undelivered for other reasons

#### ICMP Data:

- \* Messages received
- \* Messages received with errors
- \* Destination unreachable messages
- \* Time exceeded messages
- \* Parameter problem messages
- \* Source quench messages
- \* Redirect messages
- \* Echo requests
- \* Echo replies
- \* Timestamp requests
- \* Timestamp replies
- \* Address mask requests
- \* Address mask replies
- \* Messages attempted to send
- \* Messages failed to send

#### **VTAM Performance Data:**

- \* VTAM Agents monitor performance of VTAM applications and devices, including:
- \* Numbers of PIUs transmitted to and from applications and terminals
- \* User, host, and network response times
- \* All logical units in session with VTAM applications are monitored, including switched logical units communicating via NCPs
- \* Session details for individual terminals describe virtual sessions, i.e. traffic between session managers and applications. The data includes:
  - \* transmission, response, and relay times for terminals, session managers, networks, and hosts
  - \* number and size of PIUs sent to and from applications
  - \* details for each virtual and explicit route
  - \* Buffer pool data describe the size and capacity of VTAM buffer pools.
- \* Application availability statistics, collected through VTAM's API interface, report on down-time and the portion of time that applications are available to users.

\* Response times for VTAM sessions are measured with the dynamic definite response protocol (DDR). Messages from VTAM to devices include an order for a response. When the response arrives, VSV calculates the transmission time for the original outbound message.

### **NCP Performance Data:**

\* NCP Agents monitor activity of IBM Network Communication Programs and all the devices and traffic associated with them, in all common configurations, new or old.

\* NCP summary reports show CCU utilization, NCP buffer counts, and intermediate and hold queue depths. The summary display leads to details regarding the performance of cluster controllers (or PUs), the lines from the controllers to the NCPs, and the terminals (or LUs) connected to the controllers.

\* Frame/relay reports provide data on physical and logical connections, and physical and LMI stations.

\* Ethernet LAN connections are monitored for frame counts, queue lengths, congestion, and collisions.

\* Network token ring interfaces (NTRI) physical and logical lines are monitored for TIC use, queue lengths, time-outs, frame counts, congestion, and active connections.

\* X.25 network packet switching interfaces (NPSI) are reported with detail displays for lines, for packet traffic to and from physical units, and for traffic to and from X.25 terminals over virtual circuits.

\* Session and gateway statistics describe traffic between session partners in a given NCP domain and traffic between session partners in remote NCP domains, respectively. VitalSigns monitors PIUs passing to and from VTAM applications, along with details regarding individual applications and secondary logical units (SLUs) in session with VTAM applications.

### **System Requirements for VSV**

VitalSigns for VTAM requires the following:

\* z/OS or OS/390

with IBM's TCP/IP 3.2 or higher

and with SNMP 1 or 2

(a VM version is in development)

\* VSV connects to TCP/IP via an application programming interface

\* APF authorization for the VSVLOAD library (VSV will set itself as non-swappable)

\* At least 6Mb virtual memory for the VSV region

\* At least 82 cylinders of 3380 disk space, or an equivalent

\* To interface with NetView, NetView 1.3 or greater

\* To interface with NetMaster, System Center's NetMaster 2.2 or greater licensed for ANM and NEWS