SeeTCPIP for VSE

Fact Sheet(release 1.63)

Product Description

SeeTCPIP for VSE provides a detailed view and analysis tool for your CSI TCP/IP stack(s) running on your VSE system. SeeTCPIP allows you to watch network activity on your systems in real-time and produces historical charts and reports based on previous system activity. SeeTCPIP allows you to see what applications, interfaces, hosts, foreign IP addresses, and connections are consuming the most system resources. SeeTCPIP also provides an interactive command interface to let you directly issue TCP/IP commands to resolve problems as they occur. SeeTCPIP provides a rich, friendly user-interface allowing users with varied expertise to benefit and successfully monitor your VSE systems.

Features

Monitor Highlights

- Network activity/efficiency and client counts filtered by protocol/port (IP,TCP,UDP,ICMP,Telnet,FTP,HTTP,LPD,GPS).
- Misrouted, discarded, and unsupported packets
- Checksum and datagram length errors
- Rejected connections
- Individual connections filtered by foreign IP connection, inbound/outbound byte counts, retransmits, port, and more.
- FTP users, sessions, and transactions.
- Turbo Dispatcher CPU activity including Job/Step information and SIO counts.

TCP/IP Command Console

- Issue commands directly to TCP/IP, and view
- View TCP/IP command replies and messages
- Provides interactive help for TCP/IP commands and messages.

Datagram Capture Tracing

- A dataspace is created on the VSE system for storing of datagrams.
- Click a button on the PC and the data is sent to the PC and converted to .pcap format for analysis with the free WireShark utility(formerly Ethereal) for a detailed view of packet activity.

Technical Details

- (Mainframe) Must be running CSI TCPIP 1.5F or higher.
- (PC) Must be running Windows 2000 or XP.
- (PC) Stores all data and handles all user interaction, thus eliminating most overhead from the mainframe VSE system.

Release Notes

The user-interface has been significantly redesigned.
The product has been divided into two components.

1. Network communications and data collection are run and controlled silently as a "Windows Service".
2. The user-interface is a completely seperate component that runs as a "Windows Application".

This allows the user to set up all of the TCP/IP systems that they are interested in and then start the "Windows Service" once and leave it running. Once this is done, they can open and close the "Windows Application" at any time to view their system(s) activity. So as long as the the "Windows Service" is running, information is collected on all configured systems.