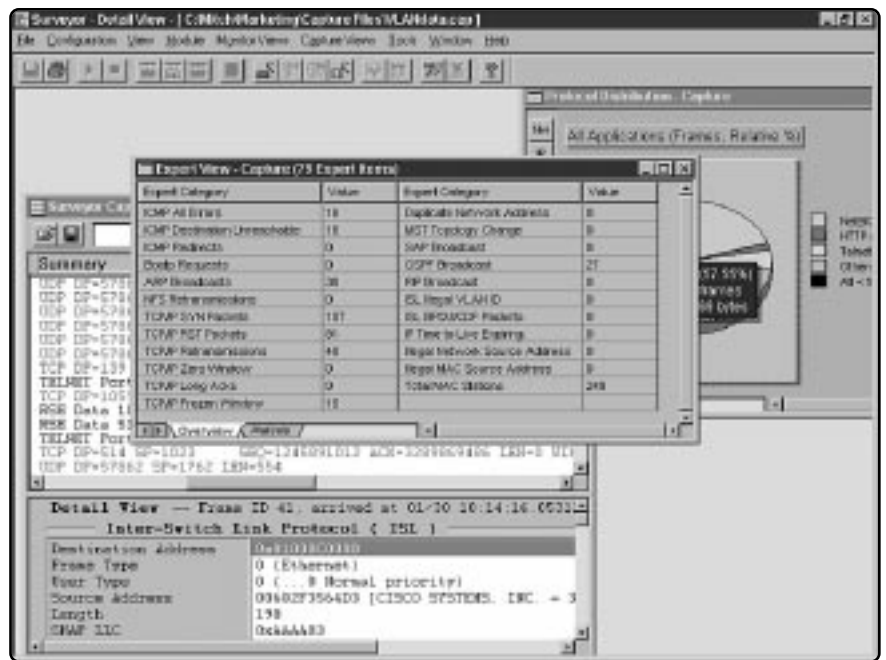


# EXPERT MODULE FOR SURVEYOR

## Automatic Symptom Detection and Diagnosis of Potential Network Problems

### Product Features

- Automatic detection and diagnosis of potential network problems allows network managers to quickly solve problems, minimizing network downtime.
- Detailed diagnosis includes user customization of probable causes and recommended corrective actions, allowing environment-specific knowledge to be leveraged, speeding problem resolution.
- Performs analysis in real-time and on capture files.
- Symptoms detected at the MAC layer through the application layer alert network managers to common network problems such as overloaded LANs, misconfigured routers and hosts, overloaded servers, and even potential hacker attacks on servers ('TCP SYN' attacks).
- Associates symptoms with their appropriate VLANs and Frame IDs and detects VLAN-specific symptoms.
- Application response time capability provides added insight into overall network behavior.



As today's networks have become more complex, troubleshooting network problems has required the network manager to develop more sophisticated skill sets. And while network management tools have become easier to use, they have also continued to provide more data than ever before. Distilling this wealth of data into meaningful information is a key objective of any network manager, allowing him to solve problems quickly, ultimately saving his corporation valuable money by avoiding network downtime.

Shomiti's Expert Plug-In is the newest addition to the Surveyor product suite. Expert automatically detects symptoms of many common and hard-to-solve network problems, provides a detailed diagnosis of the problems and then recommends corrective actions for solving those problems. In addition, Expert is highly customizable to allow the user to incorporate information and knowledge specific to his or her environment, allowing for more efficient troubleshooting. Users can actually adjust the threshold values for which most Expert symptoms are triggered, as well as customize the text that applies to each Expert diagnosis and recommended corrective action. This allows network managers of all skill levels to take advantage of Expert's powerful problem solving capabilities.

Expert information is arranged into four major categories depending on the level of detail required. *Expert Overview* provides a table of all symptoms and the number of times each symptom is detected. Symptoms are detected at the MAC layer through the application layer of the ISO model, such as duplicate network layer address, TCP retransmissions, ICMP redirects and many more. *Expert Analysis* then provides a more detailed problem description on each symptom, including time stamp and source and destination addresses. Drilling down on any one symptom will bring up an *Expert Diagnosis* which provides a detailed diagnosis of the

# EXPERT MODULE FOR SURVEYOR

problem, including a list of probable causes and recommended corrective actions. Finally, the fourth major of Expert is dedicated to application response time. Here the user can view a table of the most commonly used application protocols such as HTTP, FTP, Telnet, and more, and their associated minimum, maximum, and average response times. Just like Surveyor's capability to provide value-added information on Virtual LANs (VLANs), Expert also has the capability to associate any symptom with its VLAN identifier and can also detect VLAN-specific problems such as illegal VLAN identifiers.

Additional insight into hard-to-solve problems is provided through two new views. The first, a 'symptom-centric' host table, lists all hosts or conversation pairs experiencing a particular symptom. The second, 'host-centric' view can be accessed from the aforementioned host table, allowing the user to see all Expert symptoms detected for that host, including detailed statistics about the health of that host

Expert can be run in real-time monitoring mode or on captured data. When used on captured data, the user can automatically drill down to the frame responsible for generating the symptom. In addition, Surveyor's powerful alarm management tool is extended to include two categories, Expert Alarms and Application Response Time Alarms. Like any other alarm, the user can configure thresholds on any Expert symptom or response time and define one or more actions to be taken when a threshold is exceeded, including starting/stopping packet captures, sending an email, or sending a page.

Thus Expert, when combined with Shomiti's award-winning Surveyor product suite, now delivers one of the industry's most powerful troubleshooting and management tools for keeping your network up and running smoothly.

## Technical Specifications

Shomiti Systems Incorporated

1800 Bering Drive

San Jose, CA 95112

1-888-SHOMITI

408-437-3940

Fax: 408-437-4041

[www.shomiti.com](http://www.shomiti.com)

email: [info@shomiti.com](mailto:info@shomiti.com)

## *System Requirements*

|                    |  |
|--------------------|--|
| System:            | Pentium class system                             |
| Memory:            | 32MB minimum                                     |
| Disk Space:        | 1.5MB  |
| Display:           | 800 x 600 (SVGA)                                 |
| Network Interface: | 10/100 Ethernet Century Media Module Versions 2, |
| NDIS:              | 10/100 /1000 Ethernet, NDIS 4/16 Token Ring      |

## *Software Requirements*

Operating System: Windows 95/98 or NT 4.x

Shomiti Surveyor Version 2.4 (Can not be installed on Portable Surveyor)



MANAGE IN THE KNOW