

Volume

6

SUPPORTING THE CONVERGED NETWORK

Mark A. Miller, P.E.
President
DigiNet Corporation

A technical briefing from:



July 2002

Table of Contents

Executive Summary	i
1. The Challenge of Supporting Converged Networks	1
2. Meeting the Challenge — the Sniffer Voice Expert Analyzer	3
3. Series Summary	12
4. Acronyms and Abbreviations	13
5. About the Author and Sponsor	14

Executive Summary

This is the sixth of six technical briefing papers that examine the concepts, operation and analysis of *converged networks* — networking infrastructures based on the Internet Protocol (IP) and designed to support voice, data, video and other types of information flows. This paper addresses some of the challenges that occur when supporting converged networks, and illustrates how the *Sniffer*® Voice Analyzer from Sniffer Technologies can assist with these challenges.

Converged networks can be challenging for a number of reasons. First, the end user expectations are high, as most experiences with the Public Switched Telephone Network (PSTN) are positive and the reliability of that network is well known. A converged network is therefore, expected to perform at least as well as the PSTN.

Second, the converged network is comprised of both local area network (LAN) and wide area network (WAN) elements, which demand network management expertise in both technologies. Many network managers are experienced in one but not both areas, and therefore network management tools must bridge this gap.

Third, unlike most data networks, converged networks carry real-time traffic, such as voice and video. This real-time nature requires greater attention to network operating characteristics, such as end-to-end delays, that in most cases are more stringent than typical data applications. Once again, appropriate network management tools can assist the network administrator in achieving these requirements.

Finally, IP was originally designed to carry data — not voice or video — and, as a result, additional protocols must be used to supplement the IP functions. These additional capabilities include call establishment and termination, real-time information transport, and quality of service monitoring. Most of these supplementary protocols have been designed within the last few years, therefore most network managers are not as familiar with their operation. Once again, appropriate tools can assist the network manager and increase the likelihood of a successful implementation.

Examples of these challenges, illustrated with solutions from the Sniffer Voice Analyzer, will be presented in this paper.

1. The Challenge of Supporting Converged Networks

Supporting converged networks, which integrate voice, data, video, and other types of media into a common infrastructure, can be challenging for a number of reasons. First, the end user expectations are typically quite high. This is largely due to the quality of the Public Switched Telephone Network (PSTN) and its long-standing reliability objective of 99.999% — a factor that translates into two hours of downtime in forty years of operation. End users know from experience how reliable the telephone network is, and will accept nothing less from a network that is replacing their existing voice services.

Second, the converged network incorporates elements from both packet and circuit switching technologies, meaning that network managers must have expertise in both of these infrastructures. This requirement is counter to the way most enterprise networks have been managed in the last few years. Many organizations developed separate staffs to manage the Local Area Networks (LANs) and the Wide Area Networks (WANs), and the rapid rate of growth and change precluded much staff cross-training from one area to the other. Thus, the individuals that were expert in configuring the routing tables were not likely to know much about the T-1 or frame relay circuits, and vice versa. To successfully manage a converged environment, a very knowledgeable staff, with access to both LAN and WAN troubleshooting expertise, is essential.

Third, converged networks carry real-time traffic, such as voice and video. These applications place operational constraints on the network that may not be present with infrastructures that are strictly supporting data applications such as file transfers and email. For example, voice traffic quality degrades when the end-to-end delay exceeds established benchmarks — a constraint that might not affect email applications in the least. In order to assure that this level of operational support for real-time traffic is available, some means of monitoring and measuring these real-time network statistics is required.

Finally, the converged network includes protocols designed to augment the data carrying functions of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), and to include multimedia signal transport (see Figure 1 and review Paper 2 in this series, *Protocols for the Converged Network*). These additional protocols can be divided into three general categories: those developed by the International Telecommunication Union — Telecommunications Standards Sector (ITU-T), those developed by the Internet Engineering Task Force (IETF), and those

from vendors, such as the Skinny Client Control Protocol (SCCP) developed by Cisco Systems, Inc.

The protocols developed by the ITU-T are part of an umbrella standard known as H.323, which specifies packet-based multimedia communication systems. Protocols that are part of the H.323 suite include:

- H.225 Call Signaling which establishes, maintains, and terminates connections between H.323-based devices. H.225 signaling is based on the ITU-T Q.931 ISDN signaling standard.
- H.225 RAS: for Registration, Admission and Status messages which are sent between the H.323 endpoint and the gatekeeper for network management.
- H.245 Media Control: which provides terminal control functions, such as those required for the negotiation of channel usage, encoding algorithm selection, and so on, between end stations.
- RTP: the Real-Time Transport Protocol, which provides end-to-end delivery services for digitally encoded voice or video information.
- RTCP: the Real-Time Transport Control Protocol, which monitors and reports statistics regarding the status of an ongoing RTP session between two devices.

Paper 4 in this series, *Managing Call Flows Using H.323* discusses the analysis of the H.323 protocol suite.

H.323 is an extensive protocol designed to support a variety of multimedia applications. For some applications, such as simple voice communication within a PBX environment, the rigors of H.323 add overhead that are not required. Cisco Systems, Inc. has developed an alternative to this H.323 complexity with the Skinny Client Control Protocol (SCCP or simply *Cisco Skinny*). With the SCCP architecture, the vast majority of the H.323 processing power resides in an H.323 proxy known as the *Cisco Call Manager*. The end stations (telephones) run what is called the *Skinny Client*, which consumes less processing overhead. Like H.323, SCCP is also responsible for terminal control and management functions.

A third control protocol, developed by the IETF and known as the Session Initiation Protocol (SIP), was designed with lower overhead requirements. Paper 5 in this series, *Managing Call Flows Using SIP*, discusses the analysis of SIP-based networks.

So, between the technical and the operational challenges, along with a number of new protocols added to the mix, the job description of the converged network manager can

become quite lengthy, and the day-to-day responsibilities quite complex. Fortunately, network analysis capabilities that address these multi-dimensional issues and thus solve many of the network manager's challenges are now available.

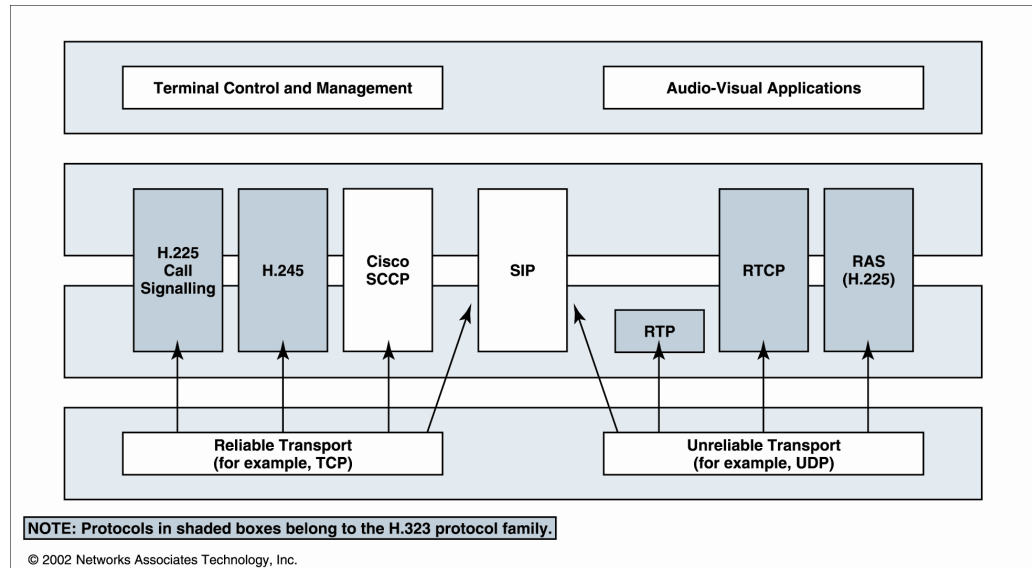


FIGURE 1. **Protocols Decoded by Sniffer Voice**

2. Meeting the Challenge — the Sniffer Voice Expert Analyzer

The challenges presented to network managers embarking on a converged network implementation — management of both the LAN and WAN sides of the network; many protocols, some of which are new to the converged environment; and the requirement to support real-time, mission critical traffic, such as voice and video — can be daunting to say the least. Fortunately, network analysis tools, such as the Sniffer® Voice Expert Analyzer, developed by Sniffer Technologies, have been developed to address these new requirements, and to assist the network manager in solving the network management challenges that result.

Sniffer Voice is a separate application that installs on top of the Sniffer Portable 4.5+ or Sniffer Distributed 4.1+ analyzer products and that enables network managers to troubleshoot, monitor, and perform expert analysis on a number of converged

networking topologies. Sniffer Voice enhances the quality of converged networks at every level and optimizes the management of voice, video, and data over a single network. With its real-time expert analysis and decoding capabilities, network managers can determine if their converged networks are delivering the toll quality voice services that their users demand. The Sniffer Voice analyzer is designed as a single tool for converged networks. It provides expert analysis for H.323, SCCP, SIP, H.225, H.245, RAS, RTP, and RTCP protocols, and also targets common problem areas such as jitter and packet loss, out-of-sequence packets, call duration, and command response times. Every packet is examined, and real-time statistics are gathered to help users spot potential problem areas that can lead to degradations in network performance.

During expert analysis, the Sniffer Portable constructs a database of network objects from the traffic that is seen. The Expert protocol interpreters learn about network stations, routing nodes, subnetworks, and connections that are related to the frames in the capture buffer. This information is then presented in the Expert display, along with symptoms and diagnoses. A *symptom* is a threshold that has been exceeded and may indicate a problem on the network. A *diagnosis* is a conclusion from the Expert that indicates that a real network problem exists. This conclusion may have been drawn from several symptoms that are analyzed together, from the high recurrence of specific symptoms, or from single instances of a particular network event. In any case, diagnoses are issues that point the network manager toward problems and solutions on the converged network.

In the Expert's model of the network, call flows and management functions occur at the Application and Session layers (Figure 2). These functions include H.323, SCCP and SIP support, plus the related protocols, as discussed above.

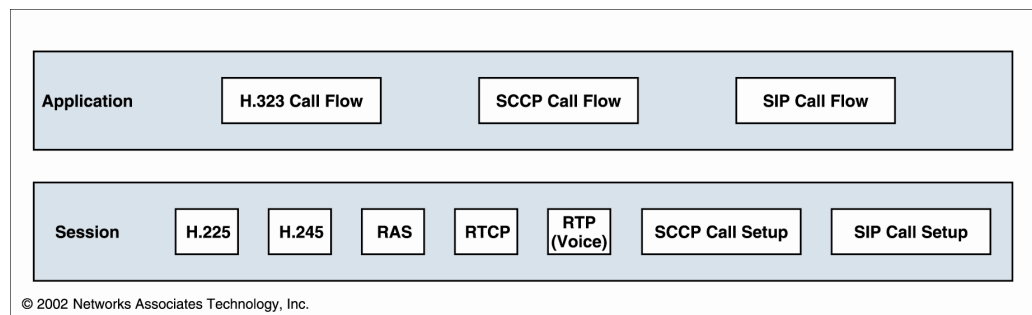


FIGURE 2. Sniffer Voice Network Objects by Expert Layer

The Expert window is one of several displays available to the Sniffer, and it is divided into several window panes. For example, Figure 3 illustrates an Application layer analysis of a call between two H.323 stations. Beginning in the upper left-hand corner of the figure and moving clockwise, the Expert window panes include: an Overview Pane, a Summary Pane, a Detail Pane, a Hierarchical Pane, and a Protocol Statistics

Pane. The Overview Pane lists Diagnoses, Symptoms, and Objects across a number of protocol layers. The Summary Pane lists each of the network objects detected by the Expert at the selected layer. The Detail pane provides further information on protocol details, as noted by the protocol in use (H.323, SCCP, SIP, RTP, and so on). The Hierarchical pane shows the network objects that are underlying a particular Application layer object. For the example in Figure 3, both RTCP and RTP are being used as part of the H.323 application under study.

Finally, the Protocol Statistics pane provides frame and byte counters on a protocol-specific basis. This information allows the network manager to determine the amount of network bandwidth that voice and video information is consuming relative to other applications that are coexisting on the network. In the example shown in Figure 3, both Telnet and VoIP H.323 traffic is active on the network, however the vast majority of the traffic is from the VoIP applications. If problems were identified with the voice calls, a quick check of the Protocol Statistics pane would indicate if the voice or video streams had not been provided with sufficient bandwidth, or if a mis-configuration of the application priorities had occurred.

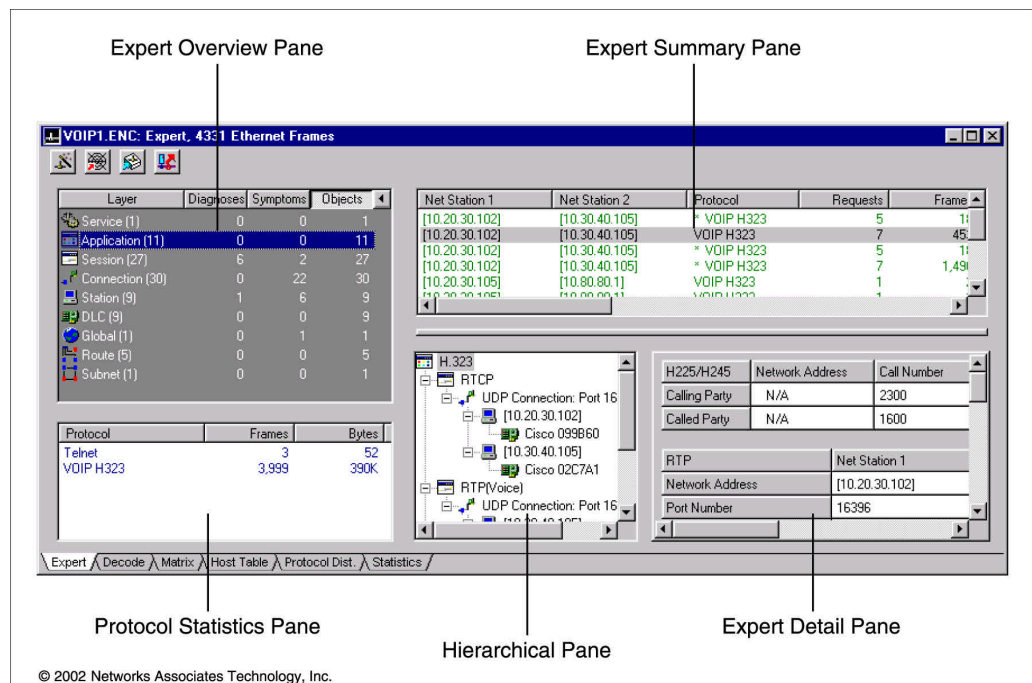


FIGURE 3. The Expert Window Panes

For SCCP-based networks, the Expert creates SCCP objects at the Application layer based on SCCP, RTP, and RTCP objects at the Session layer (Figure 4A). SCCP objects provide a means of tracking statistics related to the overall flow of an SCCP

call, including all of the underlying transactions using other protocols. The Expert then creates unique objects for a single SCCP call by extracting the Calling Party Name and Called Party Name fields from the SCCP Call Information messages (see the Detail pane).

The Hierarchical pane shows the network objects underlying the SCCP object at the Application layer. Each object can be cascaded open or closed, thus drilling down into lower layer objects. For example, the UDP objects at the Connection layer and the IP objects at the Station layer can both be examined further.

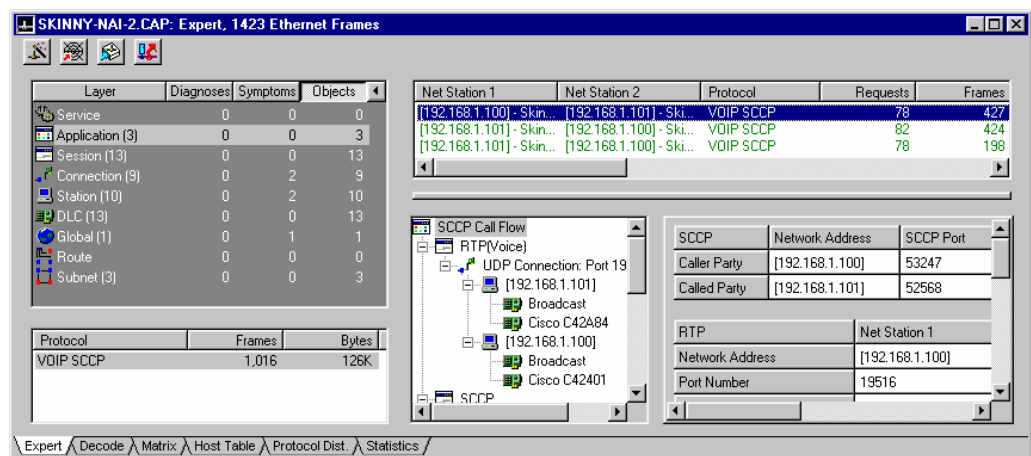


FIGURE 4A. Detail Display for an SCCP Network Object at the Application Layer

The Expert Detail pane displays the relative and delta times between end station transactions, such as communication to and from the Call Manager (CM). In the example shown in Figure 4B, the request/response transaction pairs are noted, and a relative time between transactions that exceeds 5 seconds is noted. This could identify a processing problem with the Call Manager, which may have insufficient capacity to handle all of the active end station requests for service.

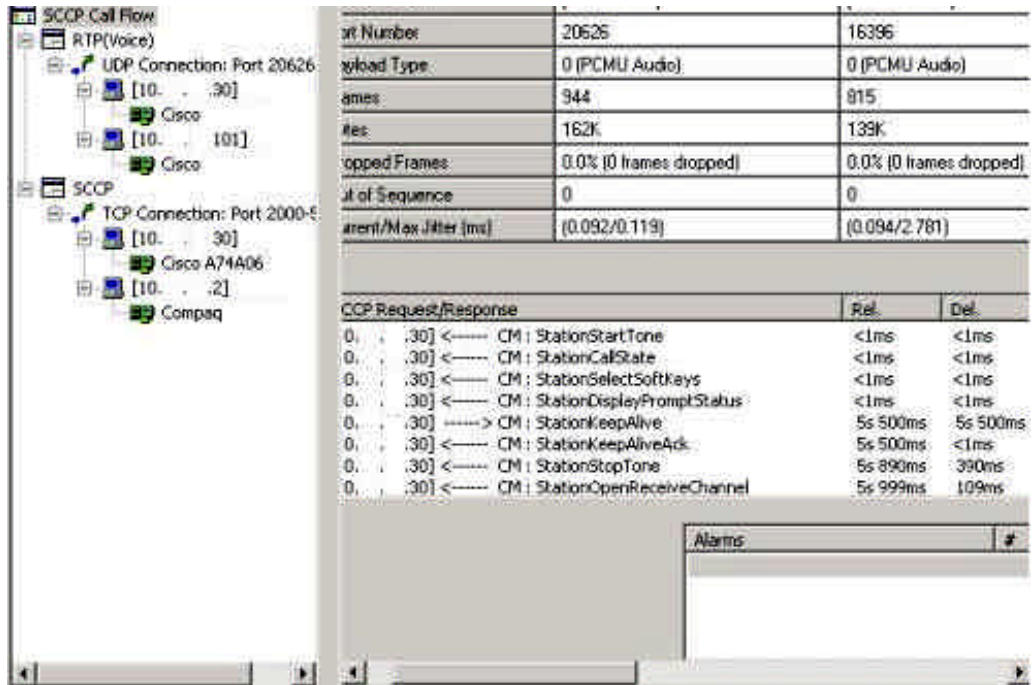


FIGURE 4B. Expert Detail Pane for an SCCP Network Object at the Application Layer

SIP objects at the Application layer are also known as SIP Call Flow objects (Figure 5A). Note that the Detail pane at the Application layer provides statistics describing the overall flow of a single SIP call, plus the underlying RTP and RTCP statistics. In addition, the Expert also creates objects for SIP connections at the Session layer, known as SIP Call Setup objects.

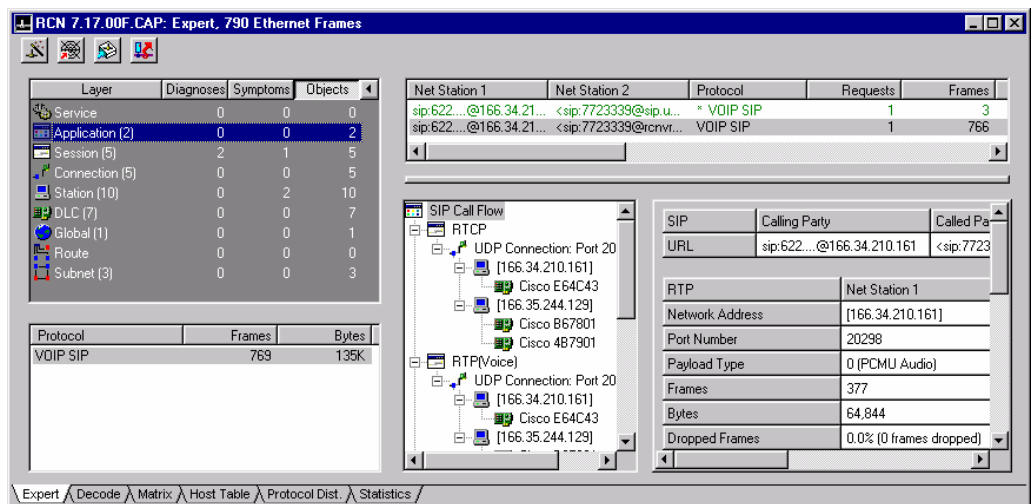


FIGURE 5A. Detail Display for a SIP Network Object at the Application Layer

The Expert Detail pane for a SIP Call Flow object at the Application layer provides SIP information that details the Calling and Called parties, plus an RTP table with statistics on the RTP transactions that are associated with this SIP call (Figure 5B). Note that the various SIP messages such as INVITE, Trying, and so on are also shown, along with the Delta and Relative time measurements between these transactions.

Of particular interest are the RTCP jitter statistics shown at the top of this pane. Station 1 Receiver Report reports no jitter, while the Station 2 report identifies 352 milliseconds of jitter. This jitter information can direct the network analyst toward a particular station that may have a mis-configured jitter buffer, thus correcting a problem on the network.

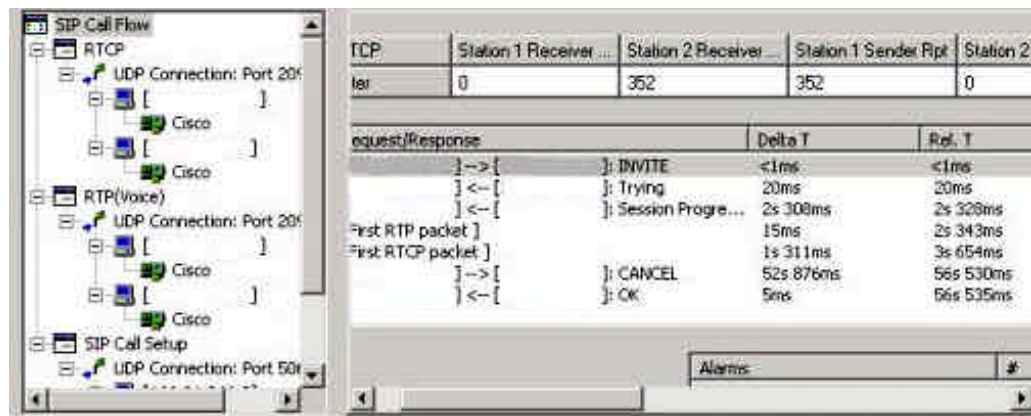


FIGURE 5B. Expert Detail Pane for a SIP Network Object at the Application Layer

At the Session layer, the Sniffer Voice Expert creates network objects for connections between stations using the H.225, H.245, RAS, RTP, RTCP, SCCP, and SIP protocols. An example of an H.225 call signaling object is shown in Figure 6. Note that a Message table is displayed in the Detail pane which includes counts of the various H.225 signaling messages (Setup, Setup Ack, Alerting, Call Proceeding, and so on) that are seen for this connection.

If you examine the Expert Detail pane in the lower right hand corner, you see the number of individual messages that have been counted. In this case, there was one SETUP message, but no corresponding SETUP ACK message. This could indicate that the station in question was not configured correctly at the Gateway, and that perhaps the access permission parameters were not set correctly.

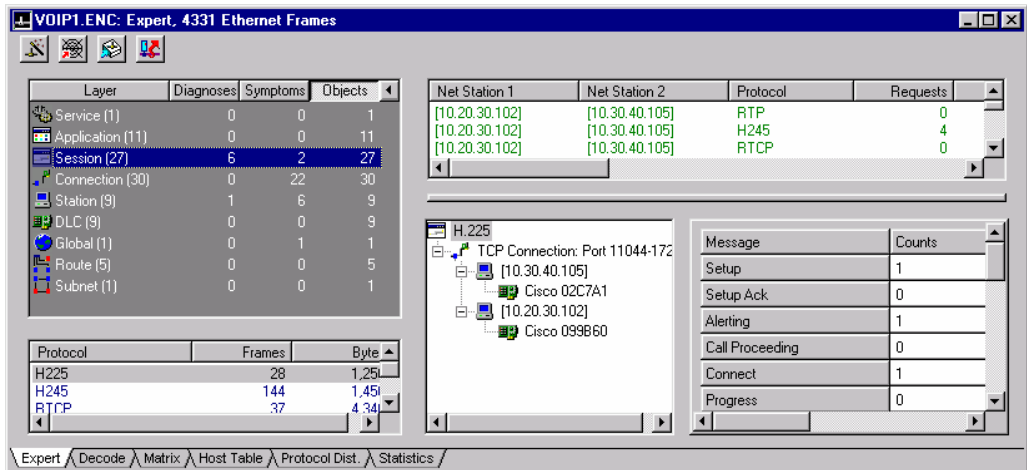


FIGURE 6. Detail Display for an H.225 Signal Network Object at the Session Layer

An example of an H.245 network object at the Session layer is shown in Figure 7. In this case, the H.245 messages are broadly grouped into four types: requests, responses, commands and indications. The Messages table indicates the number of each type of message that is seen on this connection. A Sub Messages table indicates the exact number of H.245 messages that are seen for this connection, such as the Master/Slave Determination, Capability Set, Open Logical Channel, Round Trip Delay Request, End Session, and so on.

In this example, the number of Requests and Responses are equal (both 4), indicating that the Call Manager or Gateway is responding appropriately. Further analysis at the end stations would be the next step in the troubleshooting process.

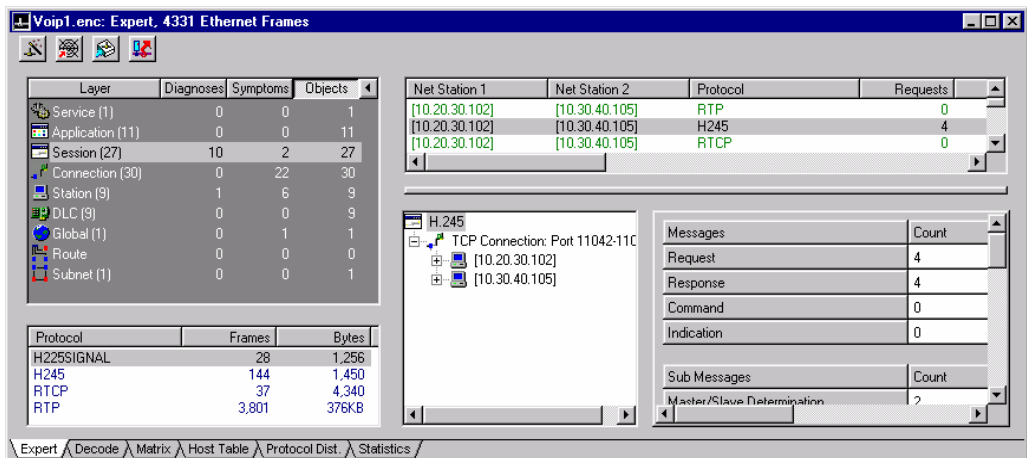


FIGURE 7. Detail Display for an H.245 Network Object at the Session Layer

Figure 8A illustrates the objects created by the Expert for a SCCP connection between two stations at the Session layer. The SCCP Info table provides identifying information for both sides of the call, the SCCP Client (or terminal) and the SCCP Call Manager. A number of additional statistics are also tabulated, including the Terminal Address, Port, Name, and Number, plus the Call Manager Address and Port.

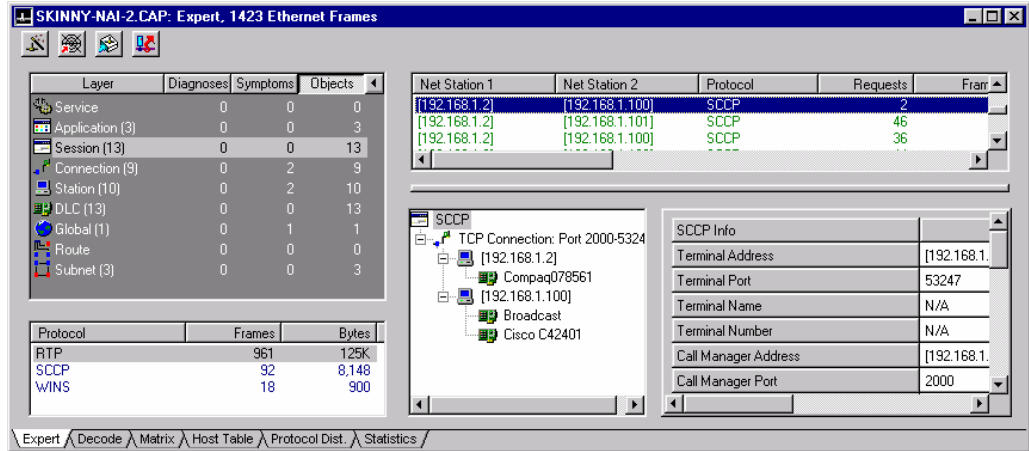


FIGURE 8A. Detail Display for an SCCP Network Object at the Session Layer

The count of the various messages sent to and from the client is displayed in the Expert Detail pane (Figure 8B). Note that the count of Keep Alive messages is zero, indicating that the call may be dropped because of the lack of client communication.

SCCP Info	
Terminal Address	[10. . .30]
Terminal Port	50283
Terminal Name	N/A
Terminal Number	N/A
Call Manager Address	[10. . .2]
Call Manager Port	2000
RTP Receive Address	N/A
RTP Transmission Address	N/A
Messages	
Message	Count
Registration/Management From Client	0
Registration/Management To Client	0
Call Control From Client	0
Call Control To Client	1
Media Control	0
Call Statistics	0
Keep Alive	0

FIGURE 8B. Expert Detail Pane for an SCCP Network Object at the Session Layer

Details of a SIP network object at the Session layer are shown in Figure 9. The SIP Methods table provides statistics on the various SIP messages (or methods) that are used for establishing, maintaining, and terminating the call. Individual statistics are listed for each method, including the Command frequency, number of Retransmissions, Round Trip Time for this SIP packet type (21 milliseconds in the case of the Invite message), the Last Response Code, and the Status, which provides a textual translation of that SIP response code (not shown in the Detail pane of Figure 9). The Last Response Code is particularly useful, as it provides an assessment of the call from the protocol's, not end user's, perspective. Thus, if a Response Code of 200 (OK) was returned, the network is operating properly.

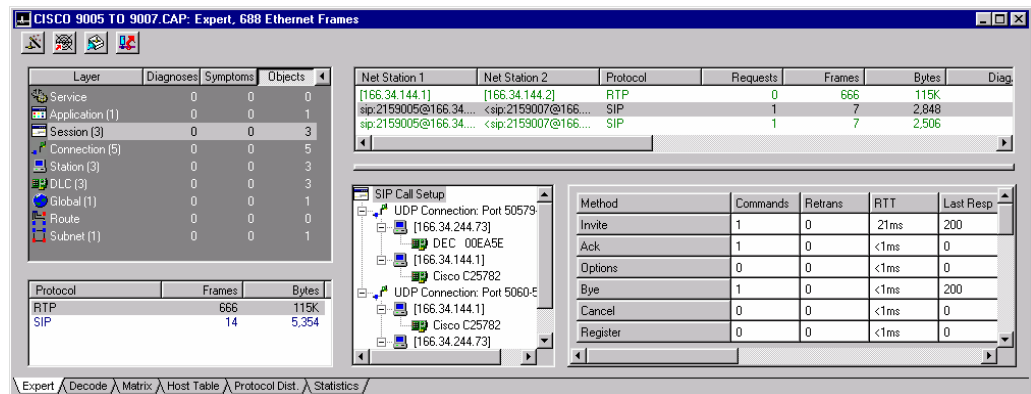


FIGURE 9. Detail Display for a SIP Network Object at the Session Layer

The Sniffer Voice also includes a number of Expert alarms that can be triggered by specific severities and thresholds. In Figure 10, note that within the Expert Overview Pane, the Symptoms column is selected at the Session layer.

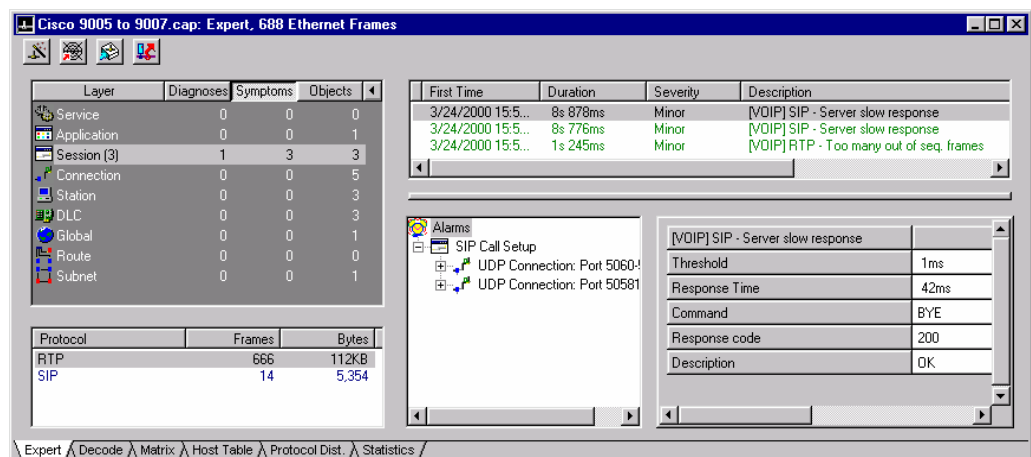


FIGURE 10. The Expert Window with SIP Server Slow Response Symptom

The Expert Summary Pane shown in Figure 10 provides a listing of all symptoms detected at the Session layer. The Expert Detail pane provides detailed information on the alarm selected in the Summary pane (a SIP - Server Slow Response symptom, plus further details regarding the threshold.

In summary, the Sniffer Voice analyzer provides the network manager with the operational details required to analyze, diagnose, and manage mission-critical converged networks. The Sniffer's expert technology bridges the gap between network manager's personal capabilities and the challenges of the new converged network.

3. Series Summary

This is the sixth of six technical briefs on Converged Networks sponsored by Sniffer Technologies. Titles of previous volumes in the series include:

- 1. Introduction to Converged Networking:** A description of concepts and challenges of converged networks, including business, technical, and operational issues.
- 2. Protocols for the Converged Network:** A look at the components of the converged network, the ITU-T and IETF multimedia protocol suites, and the protocols required by each component.
- 3. Implementing the Voice over IP Network:** Issues to consider before you jump in, including existing network utilization, planning for new applications, network design, and interoperability testing.
- 4. Managing Call Flows Using H.323:** The operation of the H.323 family of multimedia protocols, illustrated with case studies and output from the *Sniffer* protocol analyzer that show converged network operation from the H.323 perspective.
- 5. Managing Call Flows Using SIP:** The operation of the Session Initiation Protocol (SIP) and the IETF multimedia protocol suite, again illustrated with case studies and output from the *Sniffer* protocol analyzer.

4. Acronyms and Abbreviations

CCITT	Consultative Committee for International Telephony and Telegraphy
CNLS	Connectionless network service
CON	Connection-oriented network service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	Electronic Numbers
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITSP	Internet Telephony Service Provider
ITU-T	International Telecommunication Union — Telecommunications Standards Sector
LAN	Local Area Network
MGCP	Media Gateway Control Protocol
MOS	Mean Opinion Score
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PESQ	Perceptual Evaluation of Speech Quality
PSQM	Perceptual Speech Quality Measurement
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Registration, Admission, and Status
RSVP	Resource Reservation Protocol
RTCP	Real-time Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
SAP	Session Announcement Protocol
SCCP	Skinny Client Control Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

5. About the Author and Sponsor

Mark A. Miller, P.E., is President of DigiNet Corporation, a Denver-based consulting engineering firm providing services in internetwork design, strategic planning, network management, and new product development. Mr. Miller is the author of nineteen books on network analysis, design, and management. His latest book is titled *Voice over IP Technologies, Strategies for the Converged Enterprise*, published in 2002 by M&T Books, Inc., a division of John Wiley (Indianapolis, Indiana). He is a frequent presenter at industry events and has taught at the ComNet, CT Expo, Internet Telecom Expo, Network+Interop, Comdex, and other conferences. He holds B.S. and M.S. degrees in electrical engineering, and is a registered professional engineer in four states. For more information, DigiNet Corporation may be reached at 303-682-5244 or on the Internet at <http://www.diginet.com>.

Sniffer Technologies, a division of Network Associates, is a leading provider of network and application management solutions designed to ensure e-business uptime. Supporting one of the widest ranges of network topologies in the industry, the Sniffer Total Network Visibility (TNV) suite is an integrated solution enabling enterprises and service providers to cost-effectively keep their networks and applications up and running at peak performance. As one of the most trusted solutions for monitoring, troubleshooting, reporting, and proactively managing network availability and performance, the Sniffer TNV suite meets the demanding 24x7 availability requirements of e-business Web sites, Internet applications, converged voice, video, and data networks, and high speed switched and optical networks. For more information, Sniffer Technologies can be reached on the Internet at <http://www.sniffer.com>.

With headquarters in Santa Clara, CA, Network Associates, Inc. is a leading supplier of network security and availability solutions. Network Associates is comprised of three product groups: McAfee, delivering world class anti-virus and security products; Sniffer, a leader in network availability and system security; and Magic, providing Web-based service desk solutions. For more information, Network Associates can be reached at 972-308-9960 or on the Internet at <http://www.nai.com>.

Copyright

This paper is copyright © 2002 DigiNet Corporation. All rights reserved.

Limit of Liability/Disclaimer of Warranty

Information contained in this work has been obtained by the author and sponsor from sources believed to be reliable. However, neither the author nor the sponsors guarantee the accuracy or completeness published herein, and neither the author nor the sponsor shall be responsible for any errors, omissions, or damages arising out of the use of this information. This work is published with the understanding that the author and sponsor are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

Trademarks

DigiNet is a registered trademark of Digital Network Corporation.

Network Associates, Sniffer, Total Network Visibility, TNV, McAfee, and Magic Solutions are registered trademarks of Network Associates, Inc. and/or its affiliates in the United States and/or other countries.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.