Sniffer Technologies

The highest availability. The highest performance. 24x7.

ENTERPRISE MANAGEMENT

USING SNIFFER TECHNOLOGIES'

SOLUTIONS

EXECUTIVE WHITE PAPER

Sniffer TECHNOLOGIES

A Network Associates Company

Table of Contents

Introduction

Most modern enterprises depend on their network for access to internal applications and to provide an interface for their partners and customers. Network-based applications are being deployed in just about every area of business, from customer relationship management to shipment tracking and factory process control. Many companies, however, must also operate twenty-four hours/day, seven days/week and need their applications to be available at all times, especially when they are connected to the Internet. Since application problems can and do occur in any environment, a comprehensive set of tools to monitor events, locate faults, and quickly troubleshoot problems has become critical to business success.

Enterprise management can be defined as that set of activities needed to keep the enterprise's applications and networks operating at peak efficiency. In some enterprises the primary focus is on individual application availability and performance. The performance of the underlying network would be of concern only when it falls below an agreed upon service level. For other enterprises, it is the planning and optimizing of network and processing resources that is the most important consideration. In this case, the types of applications being used, the aggregate traffic characteristics, the demand for service and trends in utilization are the key factors. One common theme, however, is that business applications must continue to function regardless of component failures, processing schedules, traffic loading and configuration limitations. Enterprise management tools such as Sniffer Distributed can monitor "who is doing what to whom":

For example:

1. How much bandwidth is wasted by Napster downloaders?
2. How much bandwidth is wasted by users who listen to the radio over the internet at work?
3. How do you prove that slow application response time is not a network issue?
4. When you have a utilization spike how do you determine what the problem was so you can prevent it in the future?

When the network or a major application crashes (or even slows down), the entire company could be affected - product information will not be accessible, on-line purchasing will not function, and even e-mail delivery might be unacceptably slow. Customers can be lost forever if they must turn elsewhere for service, and operations costs increase when employees cannot get on with their jobs.

According to Infonetics Research, networked application downtime for outages and service degradations cost the companies in their study an estimated $10.8 million annually in lost employee productivity and in revenues from employees who directly generate revenue. The study also determined that the average length of networked application outages was approximately 3.5 hours per month. Tools that reduce this level of downtime by identifying the cause quickly can easily be justified for failures of applications such as online banking and airline reservations.

This White Paper examines the key requirements for enterprise management in a networked environment, especially in the area of application monitoring and troubleshooting. The elements of an enterprise management system and the various techniques that can be used to monitor and troubleshoot applications are described. Next the benefits of implementing enterprise management tools such as the Sniffer Technologies solution are identified. Finally, the advantages of choosing the Sniffer Technologies solution are examined.

Enterprise Applications

In the 1990s applications that were originally stand-alone are being linked together to take advantage of Internet protocols, to provide a more consistent user interface and to provide real-time transaction processing (see Figure 1). Electronic commerce expands this to include cooperation among applications in different companies for the exchange of purchase orders, invoices, inventory, etc. Some enterprise applications may even be hosted by an external Application Service Provider (ASP). Overall, business processes have become considerably more integrated and information-intensive, and therefore more support is needed for enterprise management.

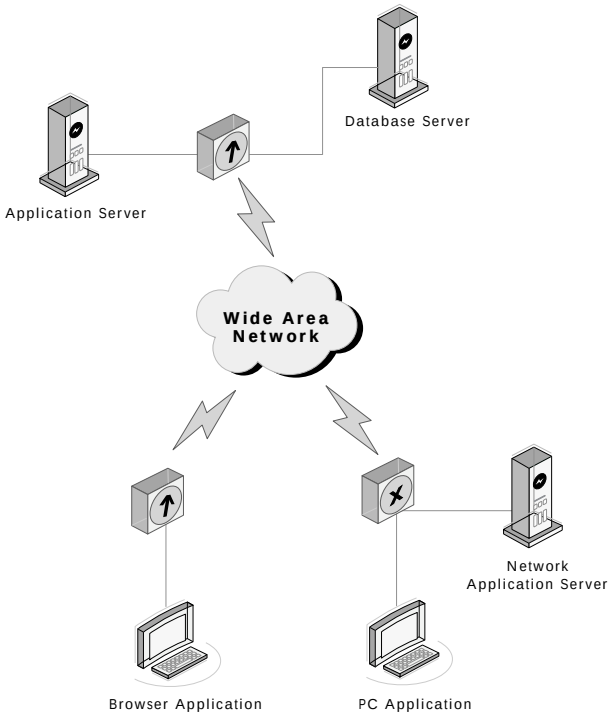

Figure 1: Enterprise Applications

Business service delivery involves three major components: servers, including the business application itself and the associated databases; networks, supporting distributed systems access and processing; and workstations, providing the human interface and local application elements. Simple request-response interactions have given way to more complex transactions involving linked transactions involving multiple servers and applications. It is important for enterprise management systems to understand how the business systems operate, how the systems are distributed, how the different network protocols relate, and what is supposed to be happening at any given time. The “big picture” is a pre-requisite for the manager to be effective in analyzing and troubleshooting application problems.

A typical example is the large financial organization that has a worldwide network built from various network technologies (Ethernet, Fast Ethernet, FDDI, etc., using TCP/IP and IPX protocols). The network on the trading floor is critical - even a few minutes outage at the wrong time could prove to be disastrous for the stock traders. Potential losses are in the millions of dollars. This network has to be monitored continuously to detect failures as soon as they occur. Historical data must also be collected for longer term performance tracking and capacity planning. In one incident, traders were unable to access an external database and were having difficulty processing their trades in a timely manner. Using the Sniffer Technologies solution, the company was able to quickly identify the problem—a server belonging to the external information supplier—and were able to take steps to resolve the problem quickly and to restore normal operations.

Another complication of modern systems is that different applications usually share system resources. In Figure 1, for instance, the Web browser and the PC application could be used for sending and receiving e-mails, for accessing inventory records or for booking orders, with each application using the enterprise intranet as the underlying network. To illustrate the problems that can arise, consider the following typical scenario:

You are closing out the end-of-quarter company books and are running the day-to-day transactions using a browser-based financial application that relies on data from an Oracle database server. Performance suddenly slows to a crawl as the deadline for the final report approaches. You know something is wrong, but what? More importantly, how can the situation be rectified quickly? Is it the desktop application, the network, the application server, or the database? Finding the source of the problem without the right tools in place can be both frustrating and time-consuming, especially when time is short and the problem is intermittent.

Applications can be located on a local Local Area Network (LAN) server, at a remote company server farm, or on a third party supplier's server. As a result, the traditional rule of thumb for network traffic has now been reversed – today, 20% of the traffic stays on the local LAN with 80% requiring Wide Area Network (WAN) access. Since almost every transaction is crossing the WAN, high bandwidth and high performance (i.e., low and consistent response times and reliable operation) have become essential. The enterprise's management systems must be able to accommodate these and many other variations in the application environment.

Enterprise Management Life Cycle

Planning, organizing, directing, and evaluating—the traditional tasks of every company's managers—have never been simple or straightforward, and this is especially true when it is enterprise applications and networks that are being managed. To be successful, an application needs to be managed throughout its life cycle, as is illustrated in Figure 2. Enterprise management includes functions that must be carried out at each stage of the life cycle.

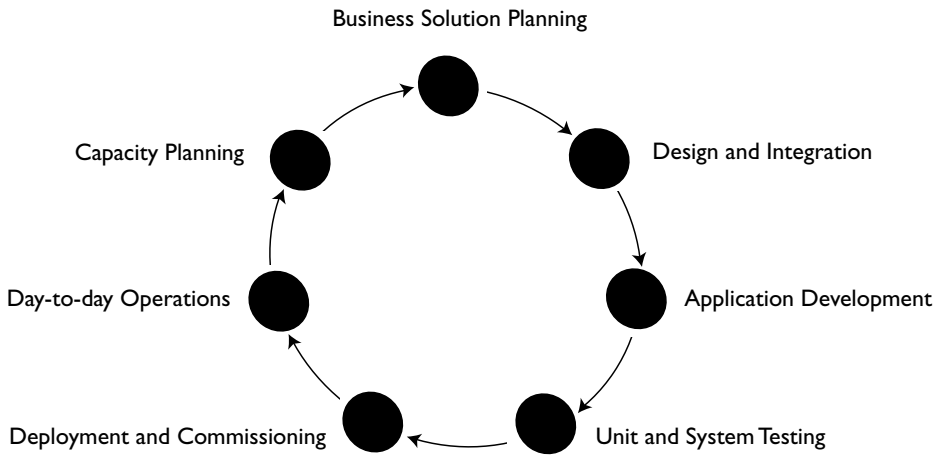

Figure 2: Application Life Cycle

It is important to be sure that the application has been designed for manageability and that it is actually capable of operating correctly. Enterprise management activities at the pre-implementation stage include the following:

• Business solution planning: The definition of management requirements such as monitoring scope and policies, troubleshooting techniques and decisions concerning quality of service, security and performance.

• Design and integration: Various management functions for monitoring and troubleshooting the application and the network including operator interfaces and collection of historical data.

• Application development: Any required links to enterprise management systems and interfaces for monitoring and analysis subsystems.

• Unit and system testing: Often a critical part of delivering a new application to its users. An application management system can be used for monitoring the testing process, for logging errors and even for simulating traffic. Since pre-production testing can be done in a controlled environment without affecting live traffic, special test cases can be used as part of the test process.

• Deployment and commissioning: Monitoring initial loads, de-bugging problems and generally watching over the performance of the application will be needed during the deployment and commissioning phase. Data gathered during acceptance testing can be used to define service level agreements and to establish performance benchmarks.

Even though there are unique challenges at each stage of an application's life cycle, it is the ability to monitor and troubleshoot application level problems that provides the greatest benefits for day-to-day business operations. Enterprise management for in-service applications has the goal of tracking significant events, especially service-affecting outages, and detecting problems as quickly as possible. Two aspects are important:

• Day-to-day operations: A number of enterprise management functions are aimed at eliminating faults. Collection of data in real-time for both the status of the network and on-going activities is an important pre-requisite. Monitoring the application for exceptions, providing operator alerts and problem detection are some of the others. Troubleshooting the problem includes verifying the failure conditions, invoking problem avoidance measures, fault isolation and resolution, and impact assessments. Operations can also include functions such as billing. Day-to-day operations should always remain focused on doing whatever is necessary to ensure the services are at their agreed to levels.

• Capacity planning: Capacity planning is concerned with the long term health of the application and the elimination of inherent design problems. The enterprise management system uses the data that has been collected for performance tracking, trend analysis, service level management, etc. This information is useful for planning resource upgrades or diagnosing systemic problems. A capacity plan attempts to minimize resource over-provisioning while also minimizing costs and meeting service level targets.

As an example of how enterprise management can support network changes, one company has a 2,000 node Ethernet network which is being upgraded to Fast Ethernet and Gigabit Ethernet over a period of six months. The Sniffer Technologies solution was used to analyze and baseline the network to assist with the deployment and commissioning of the new network segments. By deploying the Sniffer Technologies solution on key network links, the company was able to identify trouble areas and correct problems before the network was placed into full service.

Managing the Enterprise Application

Enterprise management focuses on applications and application support services (see Figure 3) but must also be closely aligned with other management subsystems. Network element management, for example, pertains to the network resources, the network operating systems and related TCP/IP services (name servers, firewalls, directory services, etc.). Since network problems can disrupt the applications it serves, there must be close coordination among the management systems. Other areas to be managed include the client-server hardware, operating systems, and infrastructure services.

Figure 3: Management Subsystems

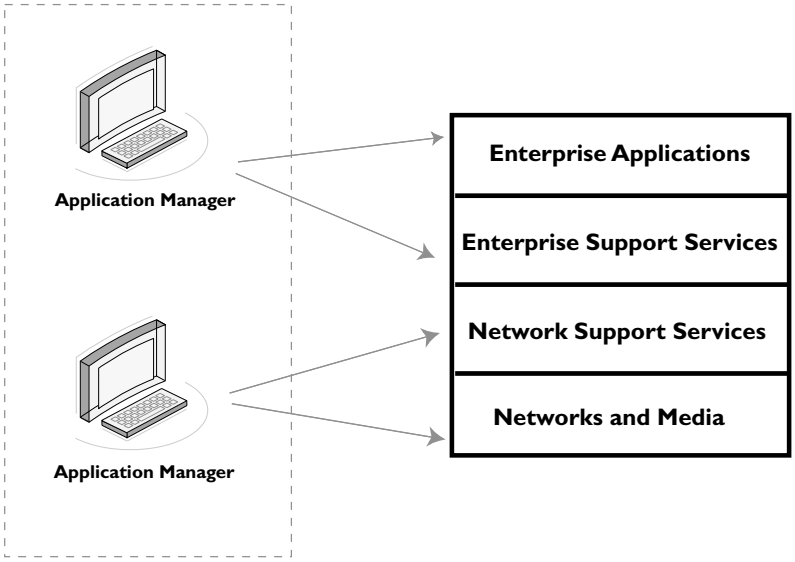

Figure 3 illustrates the division of an enterprise application infrastructure into the four areas that are described in the following:

• Networks and Physical Media: The TCP/IP protocols provide packet transfer services, with recent extensions supporting quality of service, admission controls and traffic management. Network faults are disruptive and can be difficult to diagnose, especially for multimedia, multivendor networks that are using multiple technologies and administrations.

• Network Support Services: An increasing number of network functions are implemented to support the running of the network itself. Examples include policy servers, directory services, name servers (DNS), LAN emulation servers, and security functions (e.g. RADIUS), all of which are integral to the operation of the network.

• Enterprise Support Services: Subsystems such as database servers, web servers and transaction servers provide important common components for the application. The TCP/IP architecture also defines a variety of standard application-level protocols including e-mail message transfer (Simple Network Management Protocol (SMTP) and related protocols), LDAP-based directory access, security, Web browsers (the HTTP protocol), IP telephony and file transfer. The enterprise management system must oversee these services and their interactions with the enterprise applications.

• Enterprise Applications: Enterprise applications can be divided into three categories: "off-the-shelf" applications, tailored application packages, and custom-developed applications. Application management can be used to detect and provide alarms for such events as a business component failure, performance degradation and processing errors. This helps to minimize downtime when a fault occurs. Any application breakdown is at best barely tolerable, especially when it is being used twenty-four hours per day, seven days a week but an undetected problem should be viewed as unacceptable.

The bottom line is that both the network and the applications that use it should be monitored and, when problems occur, the tools to diagnose problems should be available. For an office supply chain, for example, the Sniffer Distributed is being used for application analysis, application profiling, troubleshooting, and impact analysis. The enterprise management system supports more than 1,000 locations on a global frame relay network, a T1 backbone, an ATM backbone at headquarters and switched Ethernet LANs. In one incident a web server was frequently crashing. The problem was found by examining Sniffer traces which showed a protocol mismatch. Examination of Sniffer data for a one-user session showed that the Web server was specifying a "connection: close" in the HTML header, while the client was requesting a "connection: keep-alive." The result was continuous opening and re-setting of the HTTP connections. This is an example in which an application component was not configured correctly, an error that would have been difficult to diagnose without enterprise management support.

Capabilities of an Enterprise Management System

The enterprise management system provides a detailed understanding of an application—who is using it, when it is being used, how it is being used and what impact it has on the processing and network resources. For example, application response time can be tracked along with resource utilization and bandwidth consumption. This knowledge allows the enterprise manager to ensure that business requirements are being met by the application.

Understanding how the application operates goes beyond verifying the correct operation of a single protocol to include monitoring complete business transactions. The flow of application data should therefore be evaluated at a transaction level in addition to the standard per-packet level. For example, an Internet information request (a business transaction) often generates several secondary interactions: queries from the Web server to one or more remote databases, requests for security profiles and address look-ups are some examples of tasks that need to be performed in order to complete the transaction. All of the transaction components, any of which may cause a failure to satisfy the original request, are necessary for a successful business transaction. To do this, the enterprise management system must be able to capture and digest information about the application, the network and the events that are occurring.

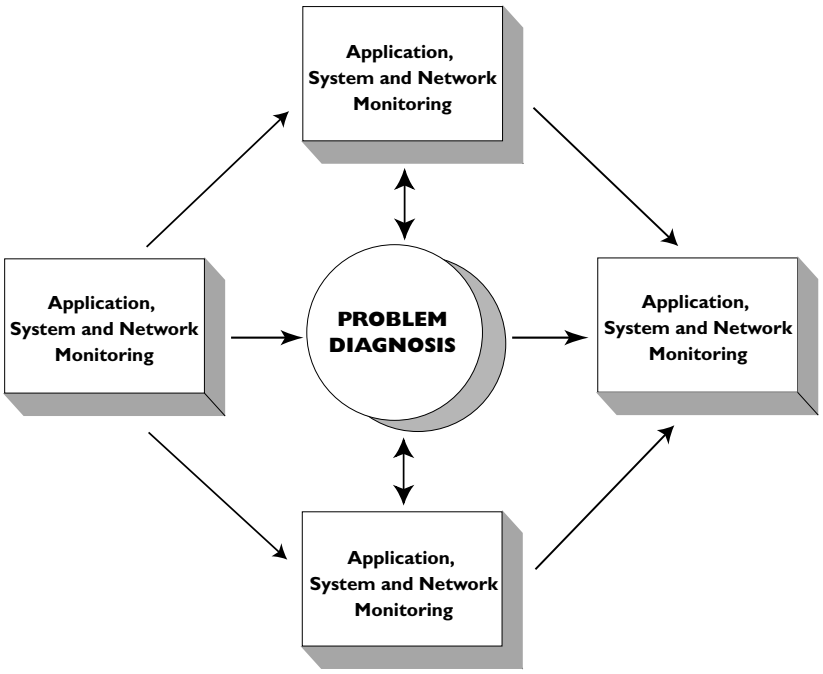

Figure 4: Enterprise Management Functional Areas

The capabilities of an enterprise management system can be divided into five major categories (see Figure 4):

1) Application Characterization

It would be difficult to know if there is a problem without knowing how the application is intended to work. Functions that can be used to characterize an application, both a priority and over time, include:

• Profiling/baselining: Profiles for traffic flows, bandwidth utilization, response times, etc. should be established to describe what is "normal" for an application. Profiles can also be used as part of a service level agreement if desired.

• Capacity planning: Application resource requirements need to be determined in advance in order to avoid performance problems. Examining usage trends, growth rates and tracking the frequency of problems such as network overloading and congestion allows proactive network planning.

2) Application and Service Monitoring

Monitoring involves the collection of data over a longer term. This data provides the basis for trend analysis and proactive management. The data looked at will range from days to months or longer. The objective is to get a long-term view of how the resources were used in the past, how they have been performing and what this may imply for the future.

Examples of the type of information that should be monitored include:

• Availability: Application availability is one of the measures used in service level agreements as a measure of performance. It is not possible to guarantee there will never be any downtime but it is important to monitor and measure all hard and soft outages. Application availability may mean the application is not usable due to significant slowdown or it may mean certain parts of it are not accessible.

• Response times: Application response time is one of the most important measures of service quality and is usually an indicator of user satisfaction. Slow response times are frustrating to the user, and also indicate problems within the network or servers. Tracking response times is necessary for proactive management.

• Transaction throughput: Throughput at the transaction level is a measure of end-to-end performance that may include multiple data transfers, linked communications among multiple servers and even interaction with external systems. Completion of business transactions in a timely manner is a fundamental requirement.

3) Problem Diagnosis (Troubleshooting)

Troubleshooting includes anything that will assist in addressing or solving an immediate operational problem. The focus is on examining what is happening now or what has just happened over the last few hours. The primary objective is to restore service to acceptable levels as quickly as possible.

The user complaint is often simply that the "business service" is not working. This must be resolved into a component failure - many problems could be the root cause, ranging from incorrect user input to network problems to temporary contention for resources. The application itself might be working well (i.e. the server has plenty of resources, etc.), but if the network is down, then the 'business service' will also be down. Problems with an application, such as a specific function that does not work, must first be identified and their source located. For example, a problem with a database server needs to be distinguished from a network link failure.

No simple, fool-proof procedure for troubleshooting exists and in many cases multiple people will need to be involved.

The data that is typically needed for troubleshooting has to be collected in real time over a relatively short period (less than a day). A network engineer, applications manager or help desk technician will typically use troubleshooting information to diagnose the problem and will then either resolve the problem immediately or, in the case of more severe problems, will devise a plan to find a resolution.

4) Problem Analysis

The most fundamental requirement is that the applications continue to be available and function correctly. The main objective of any form of management, therefore, is to restore the application to its normal mode of operation as quickly as possible. Problem resolution involves two key functions:

• Problem avoidance: Problems can be avoided or even eliminated if their underlying causes can be removed or countered. Monitoring the application and detecting trends offers the opportunity to proactively manage faults but it is usually also necessary to provide work-around mechanisms.

• Problem repair: Problems caused by hardware and circuit failures will normally be repaired by replacing a component. Software faults may be bugs in the system, which would require a program change, transient, in which case the program needs to be re-started or configuration issues. All of these require some form of human intervention.

5) Alerting and Reporting

Application management provides the mechanisms to alert managers and users to problems that may impact the operation of the application or its underlying resources. There are two major types of support:

• Application alerts: Alerts are immediate notifications of potential problems or failures requiring external intervention. Informing the manager of problems with the application as soon as they occur is an important first step in managing the service.

• Reporting: Reporting is also an integral part of an application management solution. Reporting facilitates the job of the manager by highlighting emerging issues, by digesting the large amounts of collected information and by presenting data in high level summaries that are most beneficial to the user.

Managing the application itself can be distinguished from managing the underlying processing and networking resources, although both are closely associated. Integration of the knowledge obtained from the network management system and the various application management systems would clearly be the most effective approach to enterprise management. For example, application response time, a measure of the timeliness of a complete business transaction, includes both network transit delay (monitored by the network management system) and application processing delays (which could be monitored by a server manager). Being able to recognize and distinguish among the requirements of different applications permits resource demands to be better understood and predicted.

Application Management Functions

In-service applications can be managed in different ways depending on the size, complexity and importance of the application. The three basic categories are:

• Unmanaged, reactive operation: A "hands off" approach in which the operator simply waits for a user to report a problem. Once a problem is reported, an attempt is made to find it and fix it using whatever tools may be available. Management overhead is very low but the outages could be longer and degraded services may go unnoticed. The cost of downtime may become significant if problems are frequent or are not quickly resolved. This approach is suited primarily for small networks that are not business critical.

• Active fault management: A relatively straightforward form of active management. Systems and networks are monitored either continuously or periodically in an attempt to detect and correct outages before they become visible to the user. Quality of service and performance are not typically tracked. Management overhead is higher with this approach since monitoring tools are being used but problems can be detected sooner, thereby reducing downtime. Proactive management is necessary if minimizing business disruption is a primary objective.

• Performance management: The most powerful option for enterprise management and would usually be used in conjunction with active fault management. Applications and networks are monitored on an ongoing basis with data collected and digested for both real-time fault and performance monitoring as well as for historical analysis. Proactive management of performance is the most expensive alternative but provides the benefit that many problems can be predicted and avoided entirely (such as network congestion). Analysis of trends also provides information for capacity planning and performance tuning that can minimize costs. This approach offers the best solution for large business critical networks such as online banking or airline reservations.

A number of functions are critical to the success of an enterprise management system, with the mix varying by management category. Table 1 lists the six specific areas and summarizes the options that would be available for each.

Table 1: Enterprise Management Functions

Area	Options
Message Generation	Passive (listening only); Active (messages are generated); Mixed (some messages and some listening)
Data Collection	Local (portable tester); Remote (distributed testing support).
Data Capture	Complete (all raw data stored); Digested (data is condensed to eliminate unnecessary packets); Targeted (only data for a specific application flow is captured)
Problem Detection	Continuous (probes are watching traffic continuously); Periodic (traffic is watched occasionally); On demand (data is collected only when a problem is known to exist)
Data Analysis	Manual (performed by the operator off-line); Assisted (performed with the assistance of an expert system); Automated (fully provided by an expert system)
Data Reporting	Alerts / alarms (typically provided in real-time); Online access to data; Summary reports; Trend analysis reports

No single combination of functions fit all situations. At one extreme, a portable tool is attached to a network at a trouble spot but there is no dedicated system involved. This might be suitable for smaller networks or localized networks. The opposite extreme is a fully integrated surveillance system that provides continuous monitoring of the health of the system and all its components. Dedicated instrumentation and real-time processing can be used to improve the management responsiveness, but the overall cost would be higher.

One of the most important decisions to be made is whether management control will be reactive or proactive. Reactive control involves waiting for a problem to happen, then diagnosing the problem and implementing a resolution. This may involve sending a technician to the site to install a test system after the problem has surfaced, thereby increasing outage times and the potential disruption to business operations. Proactive control makes use of on-going surveillance of the system with expert analysis to detect intermittent or growing problems that can be headed off prior to a failure occurring.

Another important decision is whether to include active testing—the generation and insertion of test messages—to measure performance. Active testing can provide excellent insights into the network and its performance, but it adds a load to the network and can therefore cause its own bottlenecks. Active testing would ideally be done with the production applications being used in a test mode so that the test is as close as possible to the actual environment. For most networks, the additional cost and complexity of this level of testing would not be warranted.

Key Elements of the Sniffer Technologies Solution

Sniffer Technologies provides a set of solutions that target towards the enterprise, field service, e-business and service provider segments. The Sniffer Technologies solutions address both monitoring and troubleshooting, allowing the user to proactively manage their applications environment. Using a Sniffer Technologies solution, the network or applications manager can see how all the system elements, from applications to databases to server links to client transactions, are behaving across multiple physical layers and topologies.

Sniffer Technologies' solutions include three main products:

• Sniffer Portable can be inserted into a network whenever and wherever it may be needed to troubleshoot problems associated with network links and switching including advanced functions such as Virtual Local Area Networks (VLANs). These devices facilitate fast problem resolution using a flexible approach to troubleshooting.

• Sniffer Distributed for in network analysis. This supports real-time troubleshooting while simultaneously collecting statistical information for historical analysis. In addition to being Remote Monitor2 (RMON2) compliant it uses expert systems for analysis and diagnosis of problems.

• Sniffer Reporting, a browser-based reporting and analysis application that include standard reports for managing service levels, controlling networking costs and proactively managing network availability and performance. Network utilization reports by application are useful for forecasting and planning.

• Sniffer Wireless designed on the Wi-Fi interoperability standard (IEEE 802.11b) and includes all the same Sniffer Portable features, plus channel surfing across 12 channels, wired equivalent policy, and support integration from the top three wireless LAN card manufacturers: Cisco Systems, Lucent Technologies (Agere Systems) and Symbol Technologies.

• Sniffer Voice provides the necessary insight into your voice traffic to address these issues and ensure that your VOIP rollout does not increase response time for other network users. It enhances the quality of converged networks at every level and optimizes the management of voice, video, and data over single network.

Physical Network Interfaces

The network interface is a key element in any network analysis tool, whether it is portable or permanently connected into the system. Support for multiple types of connectors and speeds will be required in virtually every network environment. The Sniffer Technologies solutions provide a full range of network interfaces that are suitable for most modern networks including Wireless, Frame Relay, T1 links, Fast and Gigabit Ethernet LANs, packet over SONET, and ATM.

Protocol Decoding

The Sniffer Technologies solution is able to decode a wide range of protocols covering all of the Open System Interconnection (OSI) layers, providing detailed data and analysis. Detailed decoding allows complete visibility into the network regardless of speed or topology. In addition, the Sniffer Technologies solution incorporates expert systems that automatically find and troubleshoot performance problems, providing recommendations for corrective actions to be taken by the operator.

Monitoring and Data Collection

The Sniffer Technologies solutions collect and store data for use in trend analysis and long term planning. It provides the user with a longer term view (weeks to months) of how resources are performing. This information can also be used to manage against a Service Level Agreement (SLA). The Sniffer Technologies solution includes the following facilities to assist in this activity:

a) Distributed Agents support the placement of analysis agents at key points throughout the network. This allows real-time troubleshooting and reporting of network events, and facilitates centralized management, monitoring, analysis and reporting while minimizing the amount of data flowing across the network itself. The RMON 1 and 2 data element standards are supported.

b) Simple Network Management Protocol (SNMP) and its associated Management Information Base (MIB). SNMP accesses the network elements for collecting information, for managing network activities and performance, and for solving network problems.

Expert Analysis

The Sniffer Technologies solution provides a number of “Experts,” that can be used to automatically detect, diagnose, and help to resolve problems. Sniffer Technologies’ expert functions can be used either in the on-line or off-line mode. Real-time analysis is especially useful since it reduces the time required to detect and identify problems, especially intermittent problems. Table 2 lists the key Sniffer Technologies Experts that are currently available and their principal functions.

Table 2: Sniffer Technologies Expert

Expert Area	Experts Supported by the Sniffer Pro
Routing	RIP routing protocols including tools such as Ping, Traceroute, DNS look-up and traffic generator
Database	Oracle, Sybase, Cisco, MS-SQ
Microsoft	SMB, NetLogon, Browser, MS-RAP, MailSlots, Named Pipes, MS-RPC, NETBEUI, NETBIOS (session), NETBIOS (datagram), WINS
Frame Relay	Local Management Interface, ITU-T standard Q.933 (Annex A), ANSI standard T1.617 (Annex D)
Network and Internet	TCP/IP, Novell, ATM, HTTP, IPv6, Sun NFS, X Windows, DLC, MPLS
Switch	Analyzes a switch through its ports
VLAN	VTP
ATM	LAN Emulation, MPOA, PNNI, SSCOP, Q.2931, OAM, ILMI

Operator Interfaces and Reporting

The Sniffer Technologies solutions provide an easy-to-use, "friendly" interface for both basic and expert functions. The Sniffer Technologies Experts provide context-sensitive help (called Expert Explain) for both the expert and less experienced users. These Help functions provide an aid to the resolution of existing problems.

The Benefits of Enterprise Management

Business applications can be treated as company assets. They are, however, difficult to manage especially when they are physically distributed over a wide area. Enterprise management systems provide the tools needed for monitoring and troubleshooting applications and the underlying hardware, software, and network infrastructure.

Enterprise management systems yield the following significant benefits:

a) Access to information: The real-time collection of application-related operational data provides the means to monitor current performance, collect statistics, analyze trends, and forecast future needs.

b) Problem avoidance: The customer does not want to experience problems, and the best way to achieve that is to avoid problems altogether. Proactive management allows at least some of the problems to be detected before they result in an outage.

c) Faster problem resolution: When problems do occur, the ability to react—to detect the problem and find a resolution—is key. The quicker a problem is resolved the less impact it has on the customer.

d) Performance optimization: The more the needs of the application are understood, the more the system can be optimized to satisfy those needs. System performance directly affects the quality of service from the application and this is usually customer visible.

e) Support for planning: Application baseline information can provide valuable insights for purposes of operations and service planning.

f) Management reporting: When the application is business-critical, its performance becomes important to management. Information and analysis help business managers to ensure the customer is satisfied.

g) Accounting and billing: Information can be collected that is suitable for user chargeback or billing.

Solutions from Sniffer Technologies deliver business results from the strategic use of technology which provide increased quality of service and higher staff productivity.

Summary

Business applications, servers and networks are critical to success for modern enterprises. Application downtime results in reduced productivity, lost sales and customer dissatisfaction, all of which directly impact the bottom line. Banks, for example, lose significant revenue per hour if their online systems fail, and customers will certainly leave if banking services are unreliable. Enterprise management systems can easily be justified for today's Internet-based applications that must operate on a 24x7x365 basis.

Enterprise management focuses on the operation, administration and maintenance of business applications, most of which are now highly distributed and network-centric. Identifying and resolving application problems can be a difficult and complex undertaking, requiring a solid understanding of how the application is supposed to function, the communications protocols that it uses and any infrastructure constraints that might apply. As a result, significant demand exists for enterprise management tools to assist with monitoring day-to-day operations and analyzing events as they occur.

Sniffer Technologies offers solutions for enterprise management that support distributed systems monitoring and troubleshooting and can easily be implemented today. The Sniffer Technologies solution provides all of the functions and features that are needed for successful application management including data monitoring, protocol decoding, expert analysis for troubleshooting and report generation. Sniffer Technologies offers a solution for effective application management that will reduce the time it takes to detect a problem, find a solution and restore full service.

Acronyms

ANSI	American National Standards Institute
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
DLC	Data Link Control
DNS	Domain Name Server
FDDI	Fiber Distributed Data Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ILMI	Integrated Local Management Interface
IPX	Novell version of IP
ITU-T	International Telecommunications Union Telecommunications
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MPOA	Multiprotocol over ATM
MS-SQL	Microsoft Structured Query Language
MS-RAP	Microsoft Remote Access Protocol
MS-RPC	Microsoft Remote Procedure Call
NFS	Network File System
OAM	Operations Administration and Maintenance
PNNI	Private Network-to-Network Interface
RADIUS	Remote Authentication Dial-in User Service
RIP	Routing Information Protocol
RMON	Remote Monitor
SLA	Service Level Agreement
SMB	Server Message Block
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSCOP	Service Specific Connection Oriented Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
VLAN	Virtual Local Area Network
VTP	Virtual Terminal Protocol
WINS	Windows Internet Naming Service

For more information on products, worldwide services, and support, contact your authorized Sniffer Technologies sales representative or visit us at:

3965 Freedom Circle

Santa Clara, CA 95054-1203

Tel (800) 764-3337

Fax (888) 203-9258

www.sniffer.com

4-TNV-BRC-004 4/01