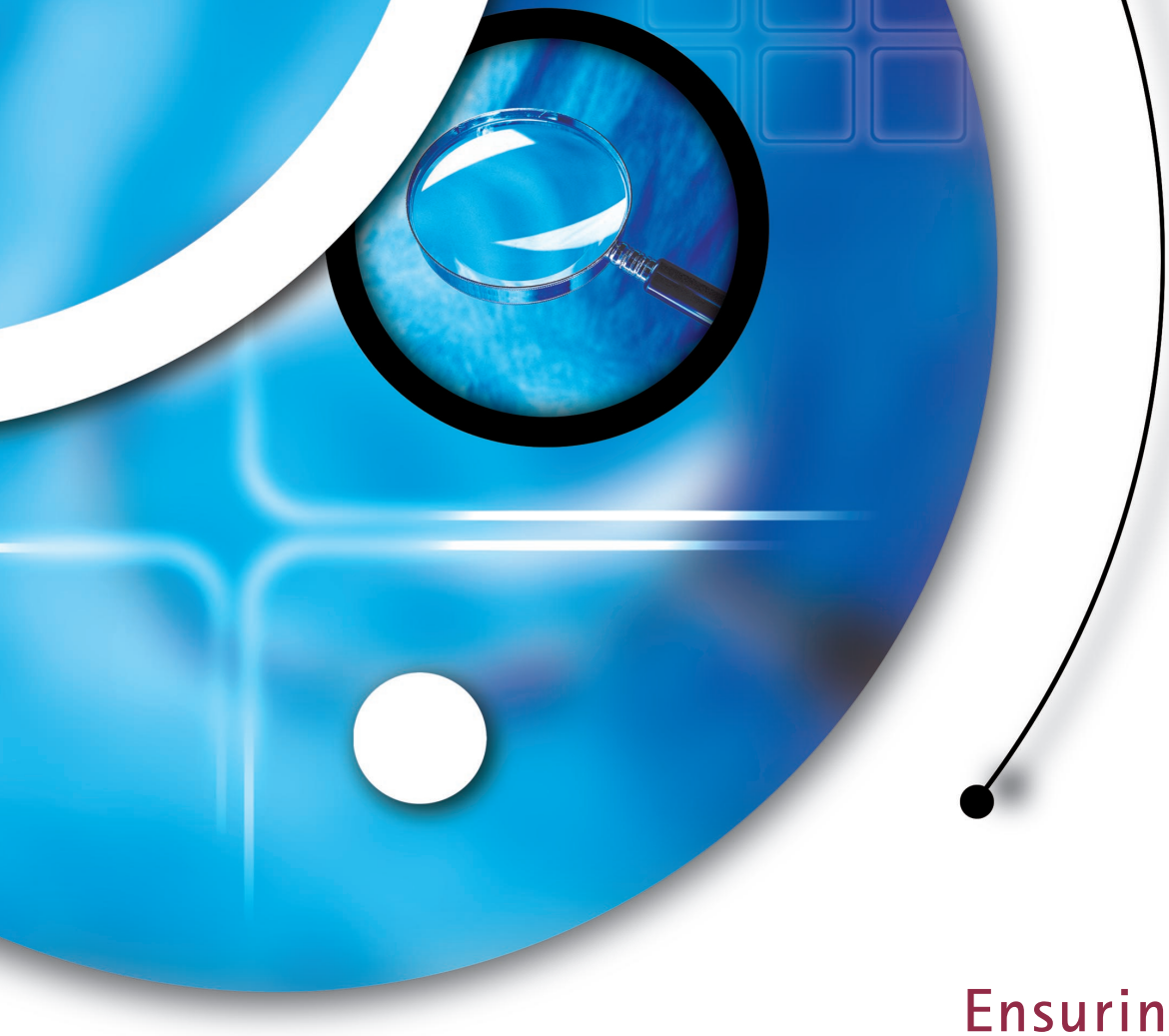


Ensuring Availability in an Internetwork Environment

SOLVING REAL-WORLD PROBLEMS

WITH SNIFFER PRO WAN

EXECUTIVE WHITE PAPER

network ASSOCIATES

Who's watching your network

Table of Contents

Overview: Definition of a New Model....2

Tracking Symptoms Down Invisible Paths....2
- Example 1: Bandwidth Utilization....2
- Example 2: Application Performance Tuning....2

Why Traditional Methods Don't Work....3

The New Model—Internetwork Analysis....4
- Entering the Cloud....4
- Optimizing the Cloud....5

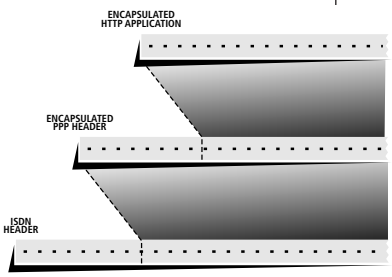
Some Real-Life Internetwork Visibility Problems....6
- Case 1: Misconfiguration Masquerades as Poor Performance....6
- Case 2: Complex ISDN Router Configurations....7
- Case 3: Welcome to New Internetwork Services....7
- Case 4: Recognizing Web or HTTP Snarls....8

The information in this white paper has been provided by Networks Associates Technology, Inc. To the best knowledge of Network Associates, these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates disclaims any and all liabilities for and makes no warranties, expressed or implied, with respect to these products, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. Distribution of these products, or information concerning these products, does not constitute Network Associates' endorsement of the products, the companies, or support services. Product information is subject to change without notice.

ENCAPSULATION

Encapsulation involves the framing of one type of communications protocol inside another protocol's headers and trailers so that the network operating system can treat the encapsulated protocol information like any other upper layer or end user information. The term to "encapsulate" is borrowed from object-oriented programming practice.

One common example of protocol encapsulation comes up whenever a link to the Internet will be handled over ISDN. Internet service providers typically support Point-to-Point Protocol (PPP) at their gateway to the public network. Point-to-Point Protocol headers and trailers must be carried as user data inside the ISDN protocols. If the PPP packets in turn carry HTTP traffic for Web browsing, then the HTTP data has been encapsulated inside PPP packets, which in turn are encapsulated in the ISDN protocol.



Protocol encapsulation hides packet headers and trailers from the network, which only deals with the frame.

Overview: Definition of a New Model

The routing of Local Area Network (LAN) traffic over a growing variety of Wide Area Network (WAN) links presents many new challenges to network management. Such links typically connect remote high-speed LANs to make one large corporate or enterprise network, either physically located in the same location or virtually connected. They may involve any of a variety of WAN transport facilities and a huge number of applications.

Network managers and engineers are using a new model of protocol analysis to monitor internetwork performance where neither a LAN nor WAN analysis approach by itself would suffice. Internetwork management requires visibility into LAN protocols when looking at an internetwork link—that is, a "WAN's-eye view" of the LAN—to optimize network operation. Internetwork analysis should include encapsulated protocol interpretation in conjunction with WAN transport performance measurement and problem diagnosis (see Encapsulation text at left).

Tracking Symptoms Down Invisible Paths

The internetwork analysis approach looks at a broad range of possible causes for almost any given symptom. The following two examples illustrate the contrast which can be found in different aspects of internetwork operation.

Example 1: Bandwidth Utilization

An important aspect of internetwork analysis is bandwidth optimization, which, in some cases, may require modifying a router configuration to filter out unnecessary traffic.

Consider the case of one company that boosted the performance of a highly utilized leased line. The network manager noticed that LAN headers and trailers were unnecessarily being routed over the WAN link. A router at the far end was removing the headers and trailers, so having this overhead filtered at the local end would lose nothing. This simple reconfiguration of the router optimized utilization of the link.

Example 2: Application Performance Tuning

At other times, internetwork analysis may uncover the need to fine-tune a critical application. Application performance can be improved by reducing overhead. Consider the credit card company who found largely identical database records being sent three times between the same network stations. The user would request a large record from a remote file server, and the entire record would be transmitted over a WAN link for display at the user's terminal.

As the application was designed, the user would ever change only one field in the record. After the user made a change to one field in the record, the entire record was sent, along with all the unchanged fields, back to the remote database server. The server then retransmitted the whole record to the end-user station for verification. Three transmissions of the entire record were used where only one was really needed.

Both cases show a clear and significant return on investment from using a WAN's-eye view of the LAN. In the first case, reconfiguring network equipment increased the capacity of the link by 25%. Network management preserved existing WAN capacity so future expansions could be postponed or scaled down.

In the second case, the network load for one stage of a critical application was reduced by 67%, dramatically improving the performance of the database and other applications, and raising user satisfaction. In either case, neither the problem nor its solution was obvious, or even visible, at first glance. To identify the problems, it took a protocol analyzer that could drill through WAN headers to provide analysis of encapsulated LAN data packets. Without the proper analysis tool, upper-layer inefficiencies are easily missed.

The process of internetwork troubleshooting—identifying problems from symptom to solution—will be hampered without the benefit of a WAN's-eye view. The network manager will increasingly find this the case as WANs become the backbone of the e-business environment.

Why Traditional Methods Don't Work

Internetwork analysis requires a wider scope of analysis methods borrowed from both LAN and WAN disciplines. To use an analogy, typical WAN analysis tools have concerned themselves only with getting the train from one end of the line to the other; it did not matter what goods the train's cars may have contained. Now, the nature of the business has changed, and network managers need to look more closely at what's inside.

Such changes reflect the convergence of LAN and WAN technologies. The emergence of Transport Control Protocol/Internet Protocol (TCP/IP) and related standards—such as Hypertext Transfer Protocol (HTTP), the language of the Worldwide Web, made widespread by the Internet and Web—have changed how corporations use networking.

The New Model—Internetwork Analysis

To uncover problems on internetwork links, network managers must deploy WAN protocol analyzers that decode above the traditional physical data link and network layers up to the application layer. The network manager must analyze both LAN applications and WAN transport. Unsatisfactory performance on internetworks may be caused not only by WAN transport problems, but also by a poorly configured application. Giving network technicians the flexibility to interpret WAN traffic in depth gives them the insight to make changes that will have significant impact on internetwork performance.

The following example illustrates how looking only at whether the train gets from Point A to Point B might blind you to a significant problem within the train's cars. In this example, a large company's sales database was being accessed by hundreds of remote users. The database server had been configured to send a requested set of records, each record in a separate frame. The records were small enough such that several hundred records could fit into one large LAN packet. By looking at the application's behavior with a protocol analyzer, the network manager was able to improve network performance by reconfiguring the server to combine several records into one packet. Had the network manager not been able to view the database traffic within the WAN "cars", this efficiency would not have been found.

Entering the Cloud

LANs typically interconnect via a WAN through multiple routers, where each router may provide any number of capabilities such as protocol conversion and address translation. These routers together make up what is known as the "WAN cloud". Conventional LAN analysis techniques alone may not help when dealing with internetwork problems which do not show up in traditional analyzers. In order to provide a WAN's-eye view, internetwork analysis equipment must be attached to physical links within the cloud. Multiple connection points may be needed (creating a situation ideal for Network Associates Distributed Sniffer System/RMON), and LAN protocol analysis techniques have to be modified to deal with new technologies and networking environments.

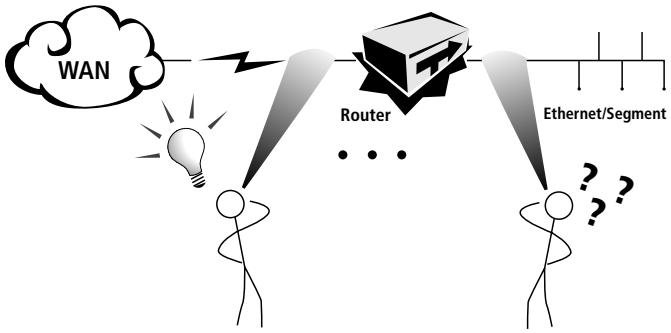


FIGURE 1

Analyzing a WAN internetwork link from the LAN side of a router (right) would be only a guessing game, but a WAN's-eye view (left) provides important details from the WAN side.

When routers connect one local network segment to another or connect a local network to a remote server, the WAN cannot be analyzed from the LAN side of the router (see Figure 1). Trying to do so would be no more than a guessing game. You cannot measure bandwidth

with certainty unless you connect directly to the WAN. Neither can you be certain which frames are being forwarded and which are simply discarded, even though you may know how your routers were initially configured.

For example, with a Frame Relay network, utilization and service capacity have to be measured from the WAN side of the router. A WAN analyzer, which can determine throughput and Committed Information Rate (CIR), allows verification of the value delivered, compared to value promised, by the WAN service supplier (see Figure 2).

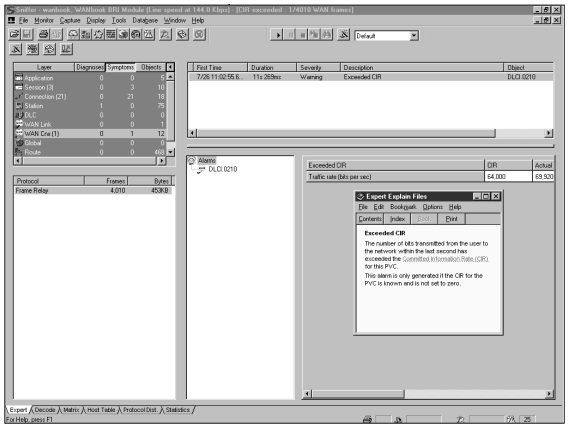


FIGURE 2
Frame Relay DLCI exceeding its CIR as called out by the Sniffer Pro WAN analyzer.

Troubleshooting WAN performance problems may be new territory for many LAN network managers, especially if the internetwork link is the only part of the network that the end user does not own outright. Problems with such links had previously been only the concern of the external link's service provider. Things have changed.

Both the end user and the service provider should assume responsibility for WAN link health. The WAN link can no longer be viewed as a pipe with a meter attached to it. Internetwork performance has to be measured in more dimensions than simple throughput. It is the responsibility of the end-user to determine whether a problem is WAN transport-related or LAN traffic-related. Once determined, there are several ways for the end user to assess internetwork performance.

Optimizing the Cloud

Bandwidth optimization of internetwork links demands that network managers expand their view to take in diverse aspects of computer networking such as:

- Configuration of address tables and forwarding databases in routers and bridges
- Verification of services provided by an outside vendor
- Client/Server application design
- Correct operation of local and remote network components

Overall throughput depends on a lot more than speed or utilization. Network managers must consider a network's applications, its end-user needs, and the operation of individual network systems—all at one time. For example, the configuration of bridges and routers depends on more than spanning tree algorithms and "shortest path first" considerations. Application behavior must be considered when judging whether a router's configuration is appropriate for any given internetwork.

TYPES OF INTERNETWORK LINKS

These typical situations reflect the use of internetworks in today's corporate systems environments.

Using the public switched telephone network (PSTN) as an on-demand or dial-up facility—for a service such as ISDN—meets the remote users' access needs (see Figure 3a). The remote link in this case is the BRI connection from the remote site through the router connecting the PSTN to the local LAN. At the remote link, a simple terminal adapter and workstation may not be sufficient. A router and a small network segment may need to be installed.

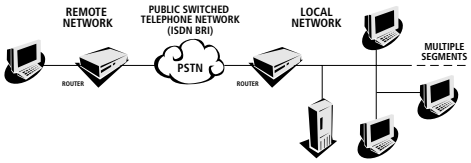


FIGURE 3a: Remote users at a small facility may be connected conveniently using an ISDN BRI internetwork link.

Another type of connection may be a private line to link a substantial remote network to the headquarters LAN using leased line, Frame Relay, or ISDN Primary Rate Interface (PRI). Both sites may have client and server elements sharing data with servers and clients at the other site (see Figure 3b).

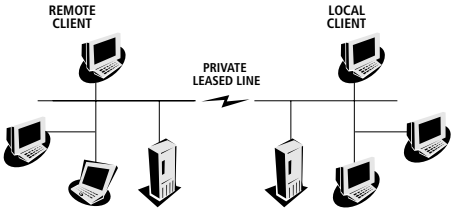


FIGURE 3b: A dedicated private or leased line would ensure constant availability of the link.

A third type of connection may be an Internet link to remote servers, providing standard HTTP, FTP, TELNET, or other services associated with the Internet (see Figure 3c).

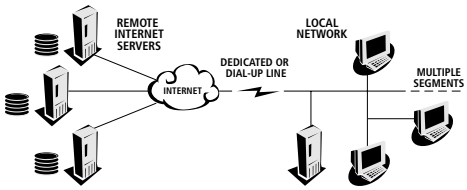


FIGURE 3c: Remote servers, such as those used as HTTP file servers, can be accessed via a dedicated or dial-up line using the Internet.

Some Real-Life Internetwork Visibility Problems

You've seen how the new model of protocol analysis works for the internetwork. Now it should be clear why traditional or legacy LAN/WAN troubleshooting techniques no longer apply. The following examples give further evidence of how you can benefit from using this new model of internetwork analysis.

Case 1: Misconfiguration Masquerades as Poor Performance

Your user population may be asking "Why is this application running so slow?" With the Internet, the question might be rephrased "Why is this browser so slow?" Indeed users may experience poor performance, and yet the root cause cannot be found by measuring WAN utilization. If a proper diagnosis is made, you may find you do not need to spend money to upgrade the WAN link after all. Internetwork analysis provides an alternative to simply adding more pipes or bandwidth to resolve a problem. Consider the following situation.

A router may send a variety of message types which are intended to keep different parts of the internetwork aware of each other. However, these housekeeping messages may load the link down with unnecessary traffic. Common examples include AppleTalk and Novell service advertisement messages (SAPs)—through which network services make themselves known to client applications—and Router Information Protocol (RIP) traffic. By identifying the source of the overload, steps can be taken to reconfigure the router. For example, a router may be configured to employ link-state routing which reduces the amount of traffic produced when new destination addresses appear.

How does the network technician diagnose root causes for symptoms that start out being described as "slow application" or "slow network"? The process can be made transparent and effortless when using expert analysis capabilities of analyzers such as the Sniffer. As shown in Figure 4 on the next page, the expert diagnosis points to a router storm which occurs when a router takes up too much capacity to share its address table with the rest of the network.

Misconfiguration errors occur more often than one might believe. Possible causes may include a router's improper initial configuration or a router's inability to receive or recognize management messages from other parts of the network. These messages may contain critical path change and user change information.

Case 2: Complex ISDN Router Configurations

Despite efforts to standardize configuration settings of Integrated Services Digital Network (ISDN) service and equipment, its complexity makes ISDN error prone and difficult to set up. Setting up remote ISDN access for a small office/home office to connect to a centrally located network requires multiple pieces of equipment and hundreds of possible parameters to configure.

Your ISDN service provider—typically the local Phone Company—cannot necessarily help with problems if they involve your local router and/or PBX configuration. The service provider usually will not spend time beyond the demarcation or network termination (the limits of the Telco's physical plant) to provide you with monitoring assistance. You may need an ISDN protocol analyzer to confirm configuration parameters.

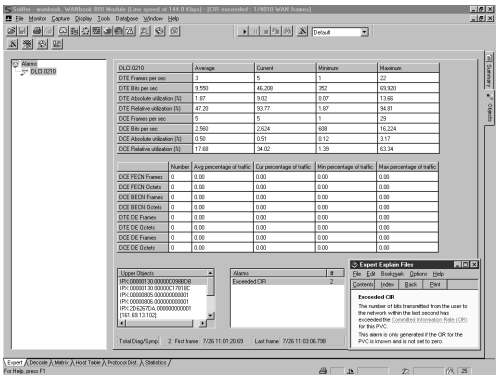


FIGURE 4

Sniffer Pro WAN's Expert diagnosis for router storms.

Case 3: Welcome to New Internetwork Services

One customer had problems bringing an ISDN Basic Rate Interface (BRI) line up, and called the phone company for help. The telco's ISDN technician checked the specified circuit from the central office switch and found the line dead. The technician assumed that the network termination device (NT1) terminating the local loop was either not connected or malfunctioning. To get a better view into the situation the technician connected a Sniffer Pro WAN analyzer to the line. The customer then picked up the line's digital phone hand-set and set it back down. On the Sniffer monitor, the technician saw a message from the central office switch clearing the call (see Figure 5). Was the NT1 malfunctioning or not connected?

Indeed, the phone company technician now had enough evidence to believe that the customer's line was connected to a switch somewhere. The question became not whether, but where. A technician was sent to examine the switch's physical connections. The newly installed ISDN BRI line had been connected at the central office, the technician found, but at the wrong punch-down block.

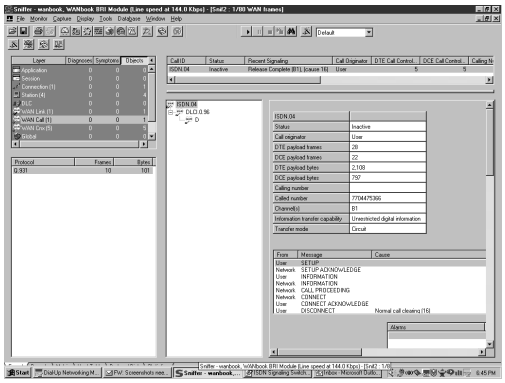


FIGURE 5

Call-clear message verifies that there is a connection to the central office switch.

Investigating even such a simple problem would have been very difficult without an analysis tool as sophisticated as the Sniffer Pro WAN analyzer. With an analyzer able to show D channel traffic, which is where B channel calls are set up and payload traffic which may combine TCP/IP and multilink PPP at one time, the problem was found quickly and easily.

Case 4: Recognizing Web or HTTP Snarls

Baselining an existing internetwork link provides an essential indicator of whether or not additional capacity should be added in response to increased throughput. How can you add capacity until you know what you have got now? Most importantly, you need to look at encapsulated protocols.

Consider the case of a company that installed a new T1 pipe only to find that its capacity was almost gone before the new facility went on-line. Demand for internetwork access to the outside world was so great that users began to complain almost immediately. Fearing a never-ending spiral, management wanted to know why the company had just paid for this expensive installation, and from the start, it wasn't enough. They asked, "Do we have to buy another high-speed T1, and if so, how many more will we need?" Surely something else must be wrong, they thought. They were right.

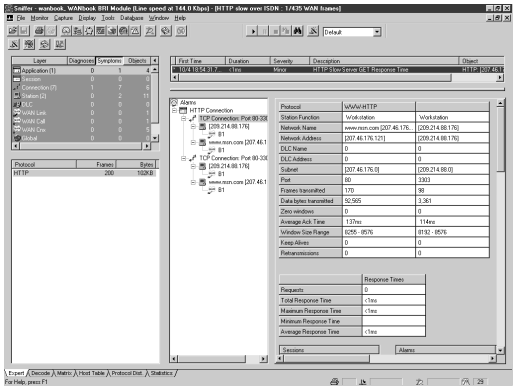


FIGURE 6

HTTP connection summary for IP addresses.

Network management personnel suspected that Internet traffic—particularly hypertext Transfer Protocol (HTTP) traffic for the World Wide Web—was the cause for the unexpected gobbling up of the new facility's bandwidth, but they didn't know how to investigate the problem or what to do when the problem was uncovered.

The network manager pored over the internetwork traffic using a Sniffer Pro WAN analyzer, and found high throughput of TCP/IP and HTTP. Further HTTP interpretation showed that much of the traffic load was what the company considered nonessential Web browsing. The Sniffer Pro WAN analyzer clearly correlated external Web station traffic to internal network users (see Figure 6). By examining the network user addresses, network management could tell that many of the heaviest Web users belonged to departments other than the one whose budget and business needs underwrote the installation of the high-speed link for Internet access. The Sniffer Pro WAN analyzer was able to document which corporate departments were using the link, so costs could be appropriately dispersed.

Only an internetwork analyzer, as thorough as the Sniffer Pro WAN analyzer can tell you what is really on your internetwork link. Had the network manager in the above situation not looked all the way up the protocol stack with a protocol analyzer that decoded HTTP traffic, he would not have seen what was really going on with the mysteriously excessive throughput.

For more information on products, services, and support,
contact your authorized Network Associates sales representative.

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (408) 988-3832*
Fax (408) 970-9727

Call for additional Worldwide Sales Offices

Visit our Website

www.nai.com

Distributed Sniffer System, Sniffer, Total Network Visibility, and Network Associates are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. © 1999 Networks Associates Technology, Inc. All rights reserved.

6-TNV-WAN-001 10/99