

Non-Intrusive Dynamic Traffic Monitoring™ for Security and Revenue

By Charlie Baker, Product Manager

Table of Contents

Abstract	3
Overview	3
Non-Intrusive Dynamic Traffic Monitoring Defined	4
Architecture	4
Network Interface Cards	5
Packet Inspection Techniques	5
Applications	5
Legal Intercept	5
QoS Management	6
Fraud Prevention.....	6
Billing	6
Additional Applications.....	6
The Brooktrout Solution	7
SMI and Bfv APIs	7
NS301 Card	7
Conclusion.....	7

Abstract

In the telecommunications world, signaling protocols provide a vast resource of databases and real-time call establishment requests containing highly detailed and useful information regarding locations, calling patterns, destinations, duration, and call frequency. To date, this data has been mined for a variety of functions from traditional call-setup to billing. Signaling traffic can also be monitored for Quality of Service (QoS), fraud prevention, legal intercept, and billing. These capabilities can greatly enhance service providers' efforts to reduce expenses, preserve capital, and retain customers. They also can provide an advantage to telecommunications vendors, giving them a powerful source from which they can build new revenues.

This white paper describes various applications that can be used to monitor and gather the information that flows across today's signaling networks in real time. These applications include targeted recording and high-speed call tracing, as well as fraud detection, QoS, and billing management. In addition, this report focuses on Brooktrout Technology's Non-Intrusive Dynamic Traffic Monitoring™ enabling technology in systems deployed in networks throughout the world.

Overview

A variety of pressures have sent today's service providers in search of new methods for cutting costs and building revenues. Factors including the erosion of the telecommunications market and U.S. economy, the downward price spiral for bandwidth, low cost long-distance, and intense competition for customers have all challenged providers' efforts to remain profitable. In addition, the convergence of voice and data, the addition of new bandwidth intensive multimedia applications, and the increasing interdependence of mobile and land line networks have increased network complexity, taxing service providers' ability to operate efficiently and cost effectively.

Equipment vendors also are affected by many of the same economic issues afflicting service providers and thus are looking for new offerings to ensure their own success. With corporate spending at lower levels than they were in early 2000, any new product that can give them an advantage over competitors will hasten them on the road to economic viability.

On the positive side, powerful technologies have emerged to help both equipment vendors and service providers solve current challenges. With these new systems, service providers can:

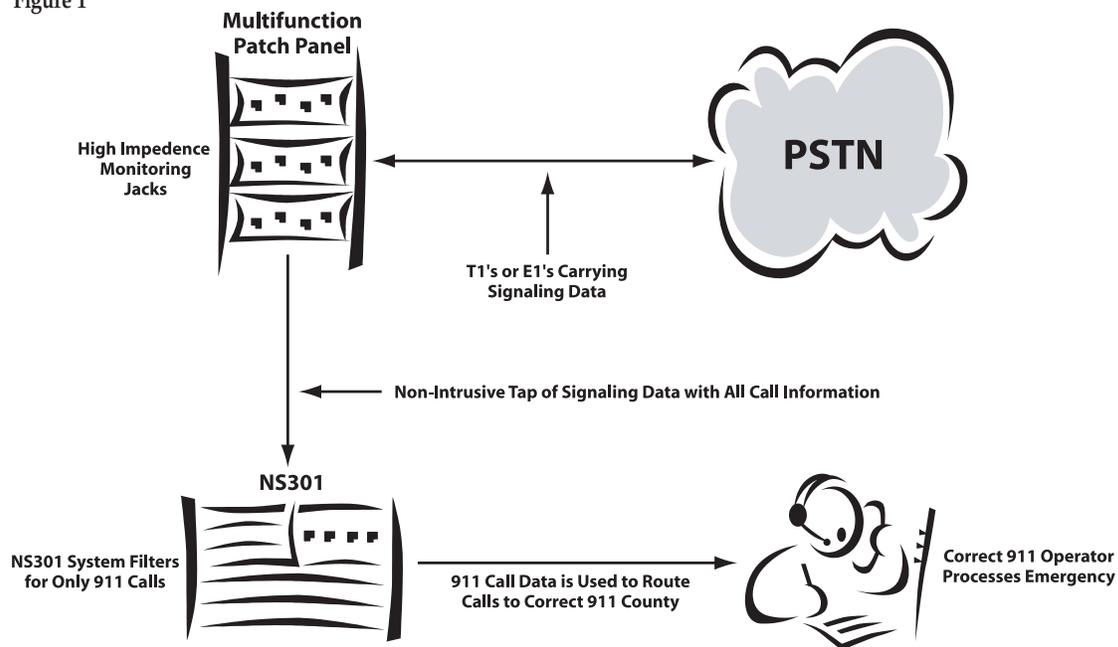
- **Improve network operations** in accordance with service level agreements (SLAs).
- **Enhance billing systems**, enabling them to charge for the exact amount of service used.
- **Prevent service fraud**, allowing them to stop a perennial drain on expenses.
- **Generate new revenues** with new legal intercept applications.
- **Meet Government requirements** for responsiveness and access.

Equipment vendors stand to provide a valued national service and possibly profit from the growing market for legal intercept applications. With today's emphasis on tighter security, new telecommunications surveillance solutions increasingly are in demand. This market will undoubtedly spark a surge in development of new systems and services as government, military, and law enforcement agencies divert funds for their expanded security efforts. However, only technology companies that quickly develop and market creative applications will maintain an advantage in this environment.

Applications that leverage Non-Intrusive Dynamic Traffic Monitoring™ exist in the network today. A quick example would be a very important public safety application in today's wireless network. The wireless network provides many challenges, especially where to route 911 calls. Getting the call routed to the correct local 911 office could mean crucial seconds in saving a life. A monitoring system is set up to receive all of the signaling information from a wireless network. There is one bit in a call setup message that identifies it as a

911 message. Board based filters can be quickly written to look only for that condition and drop all other messages. When the message is identified, it is sent to a software program that uses the rest of the information in the message to determine the cell location of the caller and the nearest 911 agency. The host-based application uses its processing resources for correlation and location and the board identifies the proper message type. The system is real-time, cost effective, scalable, and flexible.

Figure 1



Non-Intrusive Dynamic Traffic Monitoring™ Defined

The enabling technology referred to in the previous section includes hardware and software systems capable of high-speed data capture and real-time monitoring, filtering, and recording of signaling data, including SS7, ISDN, and HDLC messages. In this solution, functionality is integrated into hardware platforms, enabling signaling data to be intercepted and interpreted automatically and in real time, with no intervention by an operator or intrusion into communications. Hence, the process is referred to as “non-intrusive”. Though the technology and expertise has been around for some time, it is now being exploited to leverage data in SS7 and IP networks for use in law enforcement and business applications.

Architecture

The immense amount of signaling data traversing today’s networks is most commonly filtered, monitored, and processed with full protocol stacks, powerful servers, and large databases. This is an inefficient and expensive proposition that requires a large up-front investment in hardware and software. Such systems require complicated planning, installation, and configuration due to the complexity of the design and difficulty of moves, adds, and changes. A much more powerful solution involves the use of a packet inspection technique running on an intelligent network interface card. The “Packet Relay” function works with any HDLC based protocol, such as MTP2, to inspect packet headers and apply rules based on their content. In this approach, the physical interface boards actually have the ability to assign rules or filters to packets as they enter the monitoring system. Based on the values in the header or payload, the packets can be dropped, routed to a specific data channel for processing, copied and sent to multiple software processes, or copied and sent to multiple locations for alerting or other purposes. The application only gets the information it requires, which allows the system to scale to much higher densities for a lower initial investment.

Network Interface Cards

The high performance cards used in this solution are deployed in the service provider's or customer's network, where they are typically linked to network signaling lines via a multifunction panel equipped with high-impedance monitoring jacks or connected to a DAX from the operator. All of the signaling traffic delivered over T1/E1 lines is routed through the monitoring cards. Once target SS7 messages have been filtered from other traffic, they are forwarded to a host server for further processing.

This approach enhances performance by freeing host processors from sorting the enormous volumes of messages that traverse the signaling networks, enabling processing systems to utilize more complex algorithms and detection methods for real-time applications, trend analysis, and revenue generation activities.

Packet Inspection Techniques

Brooktrout's monitoring enabling technology utilizes rule-based packet relay technology to accomplish packet inspection. With this approach, interface cards filter packets from signaling networks and apply one or more rules consisting of a series of pattern matching tests followed by an action. During this process, specified bits within a packet are compared to a pre-determined value or database index to determine if there is a match. When the desired packet is found, a variety of actions can be taken, including discard of the packet, addition or overwriting of headers, insertion of a time stamp, redirection of the packet to an alternate destination, or duplication of the packet for distribution to multiple endpoints.

Applications

Non-Intrusive Dynamic Traffic Monitoring™ enables a wide variety of applications, including QoS, billing, and fraud prevention. These applications can be utilized by service providers to reduce expenses and improve service to customers. In addition, they can offer the transport and services necessary to perform a range of legal intercept procedures.

Legal Intercept

With the monitoring solution, law enforcement, government, and military organizations can rapidly identify and track criminal suspects, and monitor their conversations in real time, without the delays associated with legacy applications. In the spirit of Communications Assistance for Law Enforcement Act (CALEA)—a potential solution enables:

- Call tapping and monitoring
- High-speed call tracing
- Real-time mobile location information retrieval
- Call number association and profiling
- Voice channel recording
- Real-time surveillance

The solution enables authorities to establish monitoring points at key network access sites in multiple countries. Within local nodes, a system automatically analyzes a wide variety of signals on a 24-hour-basis according to pre-defined (destination or origin) phone numbers, destination country codes, or origination country codes. Retrieval of such information can allow authorities to rapidly identify callers and determine calling patterns.

In addition, mobile phone users can be tracked via the Visitor Location Register and Home Location Register systems of mobile carriers. The system can also alert authorities of the caller's specific cell location, identifying the specific cell site of the caller where further triangulation techniques can be leveraged to pinpoint the user. First level monitoring can be performed by a limited vocabulary automated speech recognition (ASR) engine to pinpoint key words and determine the necessity of further investigation. In this manner, calls can be scored based on a pre-determined grammar and ranked for further analysis. Once suspects have been identified, phone conversations can be recorded in real time without human interaction. Additionally, calls can be automatically switched to a live agent for real-time monitoring. Non-Intrusive Dynamic Traffic Monitoring can also be used to track more than just voice communications, including data, fax, chat line, short messaging, and pager traffic.

QoS Management

Because service quality is tied directly to customer churn, using monitoring to enhance QoS can be extremely valuable for providers attempting to ensure customer satisfaction and loyalty. Using this solution, providers can distribute monitoring mechanisms at multiple points across networks and at network boundaries and gateways, enabling them to gather a wealth of statistics about call patterns and behavior ranging from call completion and setup to conversation time.

Within the system, packet relay techniques determine activity of protocol layers used in network signaling, enabling providers to isolate and troubleshoot problems occurring across the network. In addition, measurement-based computation can be applied to pinpoint network congestion and anticipate other events that affect network performance. This information can be relayed to network management systems, which can be configured to generate traps and alarms.

Non-Intrusive Dynamic Traffic Monitoring™ can also be used to determine:

- SMS message counts for network sizing
- Call quality analysis and verification
- Traffic pattern analysis for routing and expansion
- Verification of customer billing claims
- SS7 link utilization

Fraud Prevention

Fraud has a direct impact on the operator's bottom line and monitoring solutions give them a tool to prevent fraudulent activity. For example, scenarios can be monitored in real time, enabling the operator to make decisions and take a variety of actions, like terminating a call before additional revenue is lost.

Using Brooktrout's monitoring technologies, providers can define filters based on use patterns, minimum and maximum bandwidth, timing, subscriber specific profiles, calling destinations, and fraudulent number associations. Filters can be updated on a frequent basis and alerts can be generated to notify personnel of a violation.

This technology can be used to block mobile calls from being connected by helping providers validate roaming callers at the home switch. Monitoring also enables providers to access registration and validation activity in SS7 networks, providing data necessary to identify suspicious activity, including counterfeit (clone) or subscription fraud.

In addition, Non-Intrusive Dynamic Traffic Monitoring can be used for:

- Pre-paid calling fraud detection, including reuse of spent pre-paid cards, or attempts to illegally recharge expired cards.
- Mobile phone fraud detection, including mobile phone cloning, real-time cloning via location and timing information, calls attempted by the same user from drastically different geographic areas within an unrealistic time frame.
- Agreement enforcement, providing a consistent user experience when a user roams between networks.

Billing

Non-Intrusive Dynamic Traffic Monitoring technology can be used for call data record (CDR), call logging and billing system inputs. It can also be applied more specifically for marketing and quality purposes. Reports indicating specific calling or called parties, failed calls, specific causes of call failure, calls handled by specific circuits, and other highly valuable information can be generated from information gathered non-intrusively from the network. Specific user patterns can be tracked based on demographics and analyzed for service penetration and average revenue per user (ARPU).

Additional Applications

Brooktrout's monitoring technology's potential uses are not limited to the applications just discussed. As the technology becomes widely pervasive, providers will apply it to a variety of new and interesting uses. For example, because monitoring can be used for real-time roamer identification, providers are already leveraging data to make contact with subscribers at the time they initiate a call, such as a welcome message or competitive service information.

The Brooktrout Solution

Brooktrout's enabling technology for Non-Intrusive Dynamic Traffic Monitoring™ is provided by sophisticated hardware and comprehensive application programming interfaces (APIs). Standards-based third party systems can easily be developed to provide value added software and services. Together, these elements provide the performance, flexibility, and control needed for today's legal intercept, QoS, fraud, and billing applications. Brooktrout's enabling technologies include:

NS301 Card

Brooktrout Technology's NS301 card is the physical T1 or E1 interface for successful Non-Intrusive Dynamic Traffic Monitoring systems. This PICMG 2.1 compliant network interface card is ready for application development. The API provides a quick time to market by allowing the straight forward commands that download the firmware, setup the time slot mapping, enable the proper protocol, and set relay rules.

Packet relay functionality, part of the API, allows developers to inspect call control packet headers at the board level and discard unnecessary messages such as FISUs, LSSUs, or user-determined packets. Off-loading the host processor enables much higher scalability for the host application and provides a more cost-effective architecture.

Additional capabilities include the ability to pass bearer channel information such as voice traffic, modem calls to the host, or recording.

Conclusion

With today's focus on reducing costs, building revenues, and tighter security, service providers are harnessing signaling messages for a variety of applications, including legal intercept, QoS management, fraud prevention, and billing capabilities.

The Non-Intrusive Dynamic Traffic Monitoring enabling technology developed by Brooktrout enables service providers and authorities to rapidly gather information about callers and calling patterns, as well as monitor conversations in real time. Using this approach, providers can build high margin revenues, save costs, and enhance QoS. Equipment vendors who are first to market with new monitoring-based products can expect to benefit from enhanced revenues, sustained profitability, and the ability to compete effectively in today's economy.



Brooktrout Technology®

Your Hook into the New Network®

U.S. Corporate Headquarters

Brooktrout, Inc.
250 First Avenue
Needham, MA 02494-2814
U.S.A.
Phone: +1 781 449-4100
Fax: +1 781 449-9009

European Headquarters

Brooktrout Technology Europe, Ltd.
Hoeilaart Office Park
Vandammestraat 5, Box 2
1560 Hoeilaart, Belgium
Phone: +32 2 658-0170
Fax: +32 2 658-0180

Sales

Needham, MA
+1 877 842-3944

Salem, NH
+1 603 898-1800

Los Gatos, CA
+1 408 370-0881

Miami, FL (Latin America)
+1 305 347-5113

Toronto
+1 416 860-6240

U.K.
+44 1344 380 280

Germany
+49 89 74120 133