White Paper

Network Monitoring and Technology Challenges

Executive Summary

Monitoring connections across a network, whether packet-based or circuit-based, can include such diverse activities as supporting network management, sending mobile subscribers location-based messages, and providing law enforcement with lawful interception capabilities. The challenges for monitoring are two-fold: capturing and storing vast amounts of data, and decoding (so that data can be analyzed) the many different data types being transported, including Instant Messaging, email applications, video streaming, and peer-to-peer connectivity, such as Skype.

This white paper presents a brief overview of network monitoring. It also discusses different network monitoring types and technologies: TDM (T1/E1, BRI, and analog), SS7 (monitoring within the service provider network), and session monitoring (IP and web). Emphasis is placed on the benefits of monitoring as an adjunct to the network (passive monitoring) or as part of the network (active monitoring). The challenges in determining data types are discussed in the context of wideband audio and video monitoring.

This white paper includes a section on Dialogic® products that are widely used to enable monitoring applications for both TDM and SS7 monitoring. Also, more information on call logging in an IP environment and call monitoring applications are provided in Dialogic application notes and technology brief.

Table of Contents

Introduction

Monitoring connections across a network, whether packet-based or circuit-based, can include such diverse activities as supporting network management and providing law enforcement with lawful interception capabilities. This white paper discusses the different network monitoring types and possible benefits that can be derived by using monitoring technologies. The types of monitoring discussed are:

- **TDM Monitoring** — Monitoring that covers T1/E1, ISDN PRI, ISDN BRI, and analog connections
- **SS7 monitoring** — Monitoring within the Service Provider Network
- **Session Monitoring (IP, Web)** — Overall session monitoring, which covers session activity from initial establishment (identification and logging on) to capturing the entire session

These monitoring types can be combined in various ways to suit the monitoring deployment desired, and they can operate in the network as active and passive monitoring.

This white paper provides a brief overview of monitoring, presents the types of network-level monitoring (TDM, SS7, and session monitoring), and uses new monitoring activities for video and wideband audio to discuss the challenges in decoding the ever-increasing number of data types.

Monitoring Overview

When discussing monitoring, some people immediately think of line tapping — or lawful interception — wherein a law enforcement agency has received a warrant or other form of permission or clearance to intercept and listen in on calls for a specific phone number. Although lawful interception does occur, this initial association may be due more to the influence of TV shows than to how monitoring occurs in reality. In the real world, monitoring is a field that supports network management, training, and subscriber services used on a daily basis. The following are some applications that monitoring supports:

- **Network Management** — Provides the ability to analyze protocol traces, statistics, and bandwidth utilization. Reports on abnormal activity or network performance issues based on assigned thresholds. Typically used within a service provider network, and alerts may be raised for manual intervention, or automated changes may take place based on preprogrammed criteria.
- **Missed Call Alerts** — Sends mobile subscribers a list of missed calls to their phone number.
- **Advertising and Marketing** — Supports location-based features, such as a user's "welcome to the network" message, triggered by detecting messages between the nearest mobile switching center register and the home location register in the user's home area.
- **Security** — Provides for analyzing video streams for changes and specific indicators, either dynamically or during post-processing.
- **Regulatory Compliance** — Provides the ability to monitor calls whether for recording and archiving, or for providing other lawful interception capabilities to law enforcement agencies.
- **Quality Monitoring** — Verifies the quality of the data stream that is being transmitted and received is within the defined thresholds.
- **Analytics** — Occurs when the data streams are rebuilt in terms of session types with the support of Deep Packet Inspection (DPI), possibly using full decode probes, and then analyzed for specific data or triggers.
- **Training** — Provides the ability for managers in a call center environment to monitor calls and provide necessary support to call center personnel, especially when being trained for the position.

Monitoring the Network

The primary type of monitoring is network monitoring, occurring when the monitoring takes place either as an adjunct to the network or as an active part of the network. Network monitoring can be:

- **Active** —an active piece of network equipment does the monitoring as part of the overall network, possibly routing or supporting the connection in some way.
- **Passive** —when data is copied and the monitoring device is not an active part of the network.

The following sections of this white paper discuss types of monitoring (TDM, SS7, and session monitoring) and how they can be combined in various ways to suit the monitoring deployment desired and how they operate in the network as active and passive monitoring.

TDM Monitoring

The main type of TDM monitoring (T1/E1, ISDN PRI, ISDN BRI, and analog) is accomplished with a High Impedance (HiZ) interface connected to the line (see Figure 1 example). A High Impedance interface needs only a small amount of current from the phone line to which it is connected, making it passive and difficult to detect. Passive monitoring allows a listener to monitor the traffic on the line without impacting the original signal.

Once connected, TDM monitoring can be used for "pen register" monitoring, which is the identification of the calling and called party numbers. More detailed monitoring can be used for:

- **Call recording** — frequently used in contact center or customer care applications where there may be some potential for dispute in the future
- **Training** — recording of new contact center agents, used to aid in training and quality improvement
- **Lawful interception** — as initiated by law enforcement to record calling behavior or conversations

During TDM monitoring, dialed digits (Dual Tone Multi Frequency [DTMF]) signaling can also be recorded, as well as the audio stream, which allows for logging (IVR) menu choices as well as subscriber phone numbers.

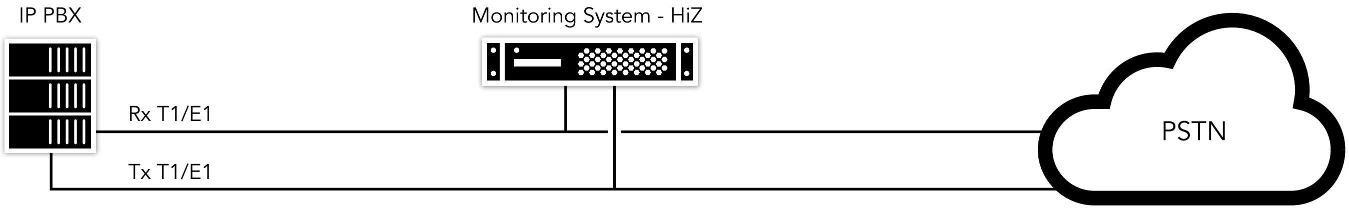

Figure 1. High Impedance TDM Monitoring Scenario

In some cases, active TDM monitoring has advantages over passive (HiZ) monitoring. In active monitoring, two call legs — one allocated to each end of the telephone connection — are bridged together. A bridged connection's advantage is that an application can take an active part in the call. This may be used for the following situations:

- Playing prompts, such as "This call is now being recorded," which a passive recording system cannot do
- Inserting DTMF or other tones
- Redirecting or stopping calls

Figure 2 shows an example of an active TDM monitoring scenario.

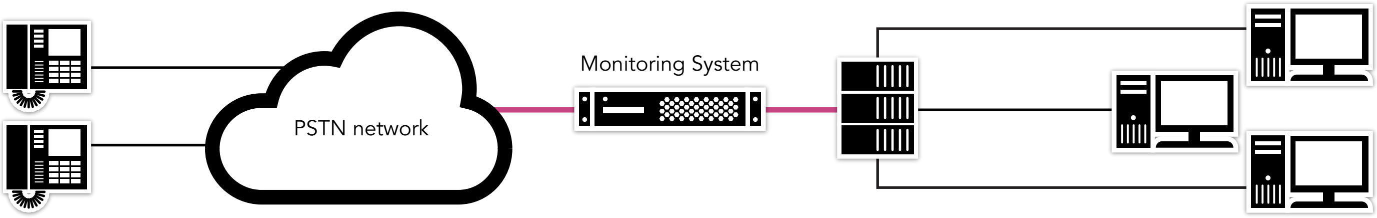

Figure 2. Active TDM Monitoring Scenario

One common active monitoring scenario occurs when a PBX duplicates calls to a dedicated T1/E1 port. The monitoring application is connected to the dedicated port and accepts calls and records them. Depending on the PBX configuration, the T1/E1 port can be just for listening or it can allow the application to also "participate" in the call. This is beneficial because complexity is reduced when duplication is done by the PBX, and the application just handles the recording.

It is usually important for a monitoring system to be able to process all types of calls. If call tapping equipment is only connected to an outside line, "internal" calls cannot be recorded. For this reason, a monitoring system may need to configure the PBX (if supported) to duplicate all calls, for example.

Digital versus Analog Monitoring

Passive monitoring on digital lines requires recording of both the RX (receive) and the TX (transmit) lines. As a result, passive monitoring systems generally utilize two TDM ports for each line being monitored. For example, a dual-span T1 monitoring board is required for passively monitoring a single T1 line. Active monitoring also requires two TDM ports for each T1 line – as shown in Figure 2, one of the two ports connects to the PBX, while the other port connects to the PSTN.

Analog lines mix the RX and TX onto one single line; therefore, tapping a phone line only requires a single port on a single-span monitoring board.

Storage Considerations

Storing uncompressed recorded phone calls in large-scale monitoring applications can quickly consume available storage. Therefore, it is beneficial to compress the recorded files (batch processing) or to record the already compressed voice streams (for example, using G.723 voice codecs) to limit the space requirements on the file server.

Monitoring IP Calls

As IP calling become more popular, there are new challenges in monitoring and recording. Two different approaches are commonly used:

- Adding IP monitoring to an existing TDM monitoring application—The migration to IP monitoring depends on enhancing the TDM monitoring application so that it may record both TDM and IP calls. This may require more work to avoid calls between TDM and IP equipment being recorded twice. To accomplish a clean monitoring solution, a change to the phone infrastructure may be required.
- Enabling an IP monitoring application to record TDM calls—Modern call monitoring applications are often based on IP equipment (IP call logging servers), but it is also desirable that the monitoring system can record TDM calls. This can be achieved by using TDM-to-IP converters (VoIP monitoring gateways) that can operate in High Impedance mode. The High Impedance monitored TDM call is converted into an IP stream that can be captured by the IP call logging system.

SS7 Monitoring

SS7 is the telecommunication protocol used to communicate between various Public Switched Telephone Network (PSTN) network elements. Monitoring in this environment can involve the monitoring, filtering, and recording of signaling data, allowing application developers to interpret events on the network and to trigger applications in the background.

SS7 signaling traffic can be carried over traditional TDM links, over ATM links, and over IP using SIGTRAN protocols. Monitoring in an SS7 network can be active or passive. If it is passive, a High Impedance interface is used when monitoring SS7 TDM or ATM links, which is similar to the interface used for TDM monitoring.

SS7 can be used for monitoring real time network traffic levels as part of network management, providing warning of abnormal activities that could affect network performance. SS7 can also be used to monitor mobile devices; for example, monitoring mobile devices crossing a city to provide information for city traffic management systems, which can then indicate changes in road traffic conditions. Also, this type of monitoring information can be provided as a "traffic watch" service charged to subscribers.

Location-based services also benefit from SS7 monitoring by allowing services to be pushed based on a subscriber's location, such as advertisements to local restaurants or activities in the area.

SS7 monitoring is also useful for fraud detection, and monitoring for common network attacks allows for intervention and prevention. SS7 monitoring may include lawful interception by recording or backhauling the data stream after using signaling events to monitor when the connection is established. Mostly though, the main driver of monitoring in this market is to enable roaming applications, such as "welcome to the network messages" or missed call alerts.

With the increasing use of IP in telecom backbone networks, it can be necessary to monitor using SIGTRAN (IP) techniques, rather than TDM. SIGTRAN, an extension of SS7, provides for using Session Control Transmission Protocol (SCTP) to carry PSTN signaling over IP. With the appropriate software, traffic of interest (such as INAP, MAP, or CAMEL) can be processed in real time to extract information such as user location and dialed digits, and to build the same set of monitoring services available for TDM. Figure 3 shows an example of a SIGTRAN monitoring environment.

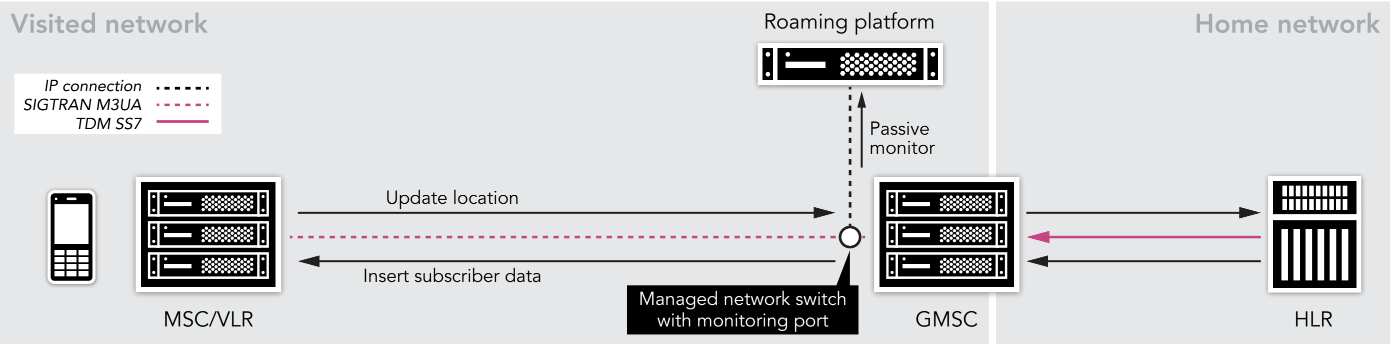

Figure 3. SIGTRAN Monitoring

Session Monitoring

Session monitoring activities (IP, web) can range from capturing the user's identification and logon when the session is initially established to capturing the entire session. Typically, a session is identified by IP addresses and the data for that session is then backhauled to a system capable of decoding it. In many scenarios, IP connection monitoring is done actively by the standard equipment being used for establishing the IP connections, but it can be done passively, if desired.

In lawful interception scenarios, the data is passed through a mediation server controlled by the service provider and then pushed to the law enforcement agency. The data passed back can be as basic as pen register data, which is the calling and called parties' identification, or as complex as to include the initial identification and logon through the entire monitoring session.

In IVR and Interactive Voice and Video (IVVR) scenarios, monitoring connections are used even if they are packet-based communications.

Figure 4 shows the numerous points in the network where monitoring can take place, be it in the enterprise or across media servers and gateways within the network, as well as the other routing equipment.

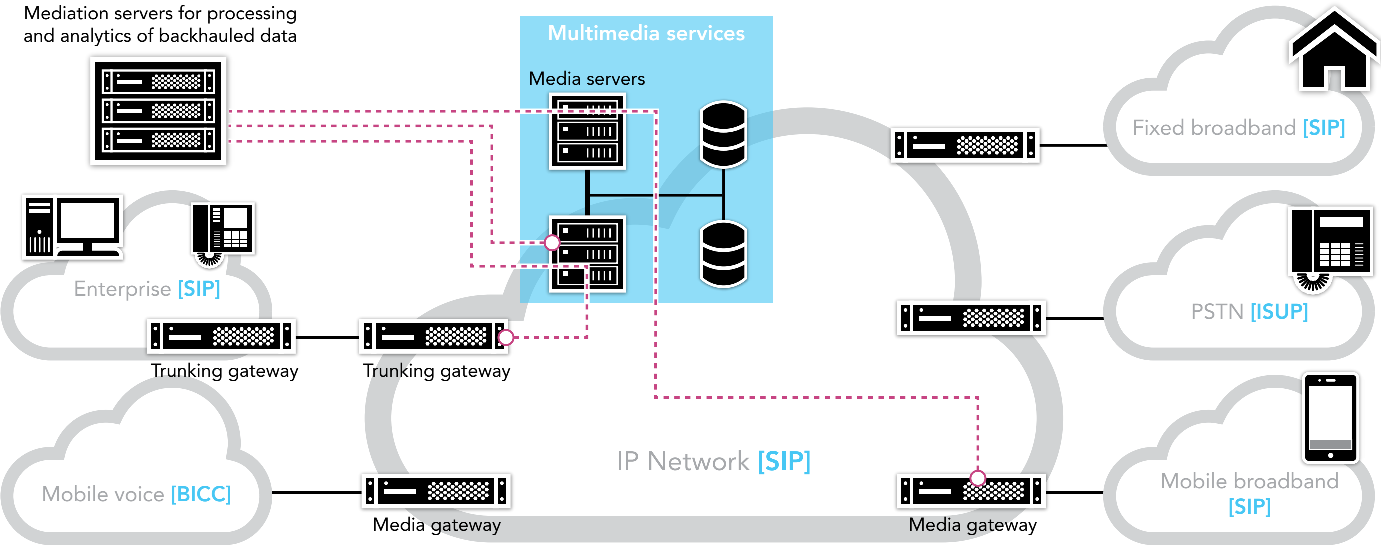

Figure 4. Monitoring in an IP environment

In next-generation networks, an active monitoring system can be employed, taking advantage of the nature of the SIP protocol. A Back-to-Back User Agent (B2BUA) can maintain two call legs, bridging them together much like in a TDM network. A B2BUA can record all of the details of the called and calling parties, and can arrange for the accompanying audio and/or video streams to be copied and directed to a recording and storage server. This kind of feature is sometimes provided as part of a Session Border Controller (SBC), providing session media and signaling that can be used by providers for lawful interception.

Monitoring the "Data Type"

The complexity surrounding monitoring involves decoding the protocols of the many different data types that are being transported from instant Messaging, email applications, video streaming, and P2P connectivity, such as Skype. Some protocols are difficult to detect, or perhaps deliberately use different ports and identifiers in order to work reliably with the widest variety of firewalls and Network Address Translations (NATs). In some cases, monitoring software must use pattern analysis techniques to handle traffic.

If the data type is not known, then Deep Packet Inspection (DPI), pattern analysis, and Full Decoding devices can be used to identify protocol types of interest and to provide the necessary decoding, if possible when the data is not encrypted. Once decoded, the data stream can then be analyzed, as necessary. Again, in addition to lawful interception, monitoring can be used to provide for the recording of a VoIP session in a call center or financial environment. The use of video in such calls is increasing, especially with Skype and other peer-to-peer type applications.

Two types of monitoring discussed next, wideband audio and video, are becoming increasingly prevalent in today's monitoring environment.

Wideband Audio Monitoring

Wideband audio (also known as HD Voice) monitoring is the monitoring of calls that are using wideband voice codecs. To monitor wideband audio calls (versus narrowband calls) requires the capability to process the relevant codec. In this sense, wideband audio is just another media type to be managed.

The challenge for monitoring wideband audio lies in the ever-increasing number of different wideband voice codecs in use. For recording applications, one option is to record and store the raw data for processing at a later time.

In some instances, the quality of a recorded call does not have to match wideband standards. In these cases, it is sufficient to convert the wideband voice stream to a standard narrowband G.711 call and record that using a standard recording system.

The monitoring solution is physically connected to the HD Voice system (for example, mobile phone system or IP traffic) at the most appropriate juncture in the network.

Video Monitoring

Video monitoring includes monitoring connections where video is part of the data stream. This can mean the monitoring and recording of a two-way video communication or the monitoring or analysis of a single video stream from a device such as a security camera, either dynamically or through post processing. The issues with video monitoring are that it adds a level of complexity on top of voice monitoring relating to the video codecs that the call is using. In an IP environment, voice calls and video calls can be monitored in the same way. The video is just another media type and, if necessary, the raw data can be stored for processing later.

However, monitoring video in a mobile world that is using 3G-324M is complex due to the challenges associated with monitoring multiplexed 3G-324M data streams. To achieve the desired results often requires using an active gateway in the chain to de-multiplex audio and video while providing monitoring capabilities, such as before converting to IP or between two 3G-324M call legs.

The areas of video monitoring that still need examining relate to the management of stored data and the analysis of the video. Storing video streams for a prolonged period of time is costly due to storage requirements. Companies that specialize in managing the data load that video storage needs often provide the ability to degrade the image over time from, for example, a high definition image to a grainer image, which takes up less storage space.

When analyzing images, being able to detect specific patterns in the video, comparable to detecting specific words in an audio stream, supports automated analysis. For example, advertisers may pay for the ability to detect logos in video.

Dialogic® Products Enable Monitoring Applications

Dialogic has a long history of providing excellent products that have been widely used to enable monitoring applications for both TDM and SS7 monitoring.

TDM Monitoring

Dialogic® Diva® Media Boards and Software

The following Dialogic Diva Media Boards support monitoring on Linux and Windows® in conjunction with the Dialogic® Diva® System Releases and the Dialogic® Diva® Software Development Kits (SDK):

- Dialogic® Diva® Media Boards

Dialogic® Diva® software products also support monitoring in many environments.

A useful summary of Dialogic® Diva® products in table format is available online.

Dialogic® CG Media Boards

Dialogic® CG Series Media Boards (PCI and PCIe form factors) can be used in passive monitoring applications where High Impedance (HiZ) support is needed. A convenient summary of CG Series Media Boards and related software in table format is available online.

Dialogic® PowerMedia™ Host Media Processing Software

Dialogic® PowerMedia™ Host Media Processing (HMP) Software with Dialogic® HMP Interface Boards (DNI Boards) can be used for TDM monitoring and active 3G-324M monitoring applications. PowerMedia HMP also supports monitoring in other TDM, IP, and hybrid TDM+IP environments, including multimedia and HD Voice applications. Different releases of HMP are available for Linux and Windows®.

SS7 Monitoring

Dialogic® MSP 1010 Multi-Services Platform

The Dialogic® MSP 1010 Multi-Services Platform is a flexible, high-density media resource platform with integrated signaling capabilities. The MSP 1010 supports a wide range of services based on SS7 monitoring, including welcome roamer, missed call alert, Location-Based Services (LBS), lawful interception solutions, and signaling services such as SMS-C, SMS Router, IN applications, and signaling converters.

Dialogic® Distributed Signaling Interface Components

The following Dialogic® Distributed Signaling Interface (DSI) Components enable SS7/TDM and SS7/ATM monitoring using distributed signaling interfaces:

- Dialogic® DSI Signaling Servers
- Dialogic® DSI SS7HD Network Interface Boards support SS7/TDM monitoring only.

The Dialogic® DSI SIGTRAN Monitor is a software product that allows SS7 message monitoring on SIGTRAN SCTP associations running over Ethernet.

If You Have Questions

Dialogic® products are used in monitoring applications worldwide. If you have specific questions about features and functions, contact your local Dialogic representative.

www.dialogic.com

For a list of Dialogic locations and offices, please visit: https://www.dialogic.com/contact.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH PRODUCTS OF DIALOGIC CORPORATION AND ITS AFFILIATES OR SUBSIDIARIES ("DIALOGIC"). NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Dialogic may make changes to specifications, product descriptions, and plans at any time, without notice.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.