

Implementing VoIP monitoring solutions

Deployment note

Introduction

With VoIP being an integral part of modern day business communications, enterprises are placing greater emphasis on the monitoring and management of their VoIP applications. In addition, as service providers and carriers strive to ensure that their services are comparable to those in the public switched telephone networks (PSTN) environment, concerns over the quality and performance of VoIP networks are driving a greater uptake of VoIP monitoring solutions among business enterprises. An analysis from Frost & Sullivan, World VoIP Monitoring Solution Markets, reveals that the revenue in this market sector totalled \$50.7 million in 2004 and is projected to reach \$297.1 million in 2008.

Quality of service (QoS) monitoring

Service providers and enterprises realise the importance and the full range of benefits that come with an effective service level agreement (SLA). Vendors offer SLAs to their customers in order to add value to their VoIP products. SLAs specify the commitment of the service provider to its customers for the minimal level of service, committing on maximum value of parameters like end-to-end latency, jitter and packet loss. Usually, the agreement also specifies exactly how long it would take to respond to trouble-tickets, and how long it would take to restore the service in case of discontinuity. Detailed escalation procedures mark a good SLA as well. Active and passive VoIP monitoring solutions are used to observe the quality of service provided to each particular customer and indicate the network details to managers in case an SLA is breached.

Monitoring for security purposes

While some organisations implement passive monitoring for quality of service and performance analysis purposes, others require this functionality to enforce security. Internal security breaches in the large enterprise are growing faster than external attacks, as institutions invest in VoIP technology. According to the 2005 Global Security Survey published by Deloitte Touche, which surveyed senior security officers from the world's top 100 financial institutions, 35 per cent of respondents said that they had encountered attacks from inside their organisation within the last 12 months. Another report from the Information Security Forum (ISF) warns that along with existing security problems associated with IP networks, VoIP will present new and more sophisticated threats, such as caller ID spoofing, voice modifiers, SPIT (voicemail SPAM) and packet injections. The ISF believes that failure to address these serious risks may bring voice communications to a grinding halt and result in identity theft and loss of sensitive information. Information moves in and out of companies in unpredictable, and sometimes frighteningly arbitrary, ways and applications are often imported and run against company policies. A secure private network is one that probably makes no assumptions about people's trustworthiness. Users are not the enemy but they are a risk. The implementation of VoIP monitoring creates a degree of accountability and transparency, and hopefully secures enterprises from internal security infringement problems.

Implementing VoIP monitoring with Aculab products

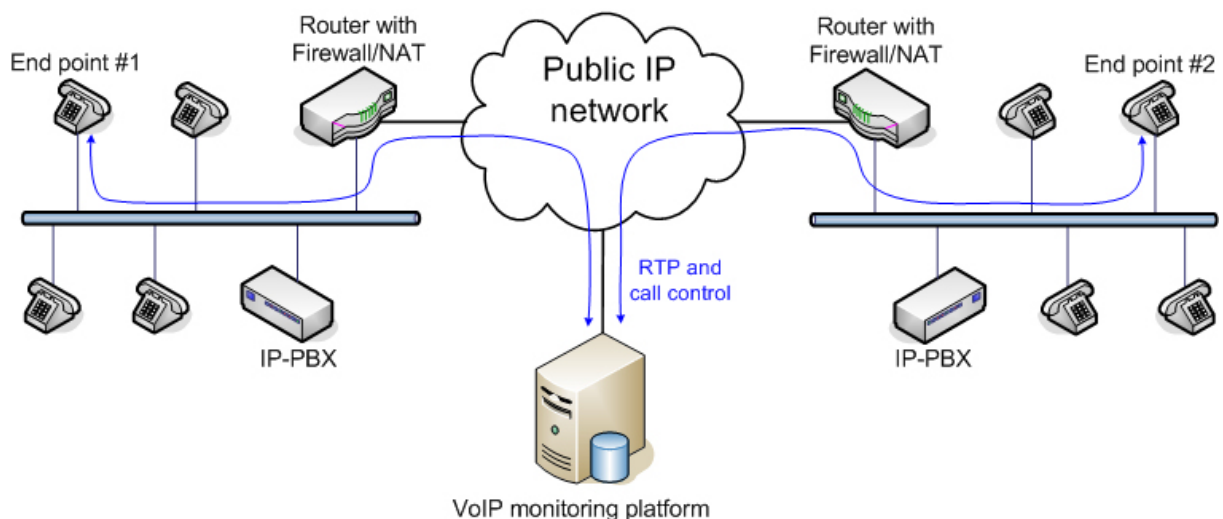
Aculab has two product categories allowing implementation of either active or passive VoIP monitoring applications. First, Prosody X PCI/cPCI media processing platforms are efficient for the creation of high channel count solutions, delivering the lowest cost per monitored channel. Second, the software-based Prosody S product, which is a host media processing (HMP) platform, provides a perfect fit for lower channel count solutions. The implementation with Prosody S requires no additional hardware. For developers looking to implement monitoring solutions in the TDM domain, Aculab offers Prosody PCI/cPCI and E1/T1 PCI/cPCI products. Therefore, our customers are presented with all the necessary building blocks to implement passive monitoring solutions for both VoIP and PSTN environments.

Solution architectures

VoIP quality management includes active and passive approaches. Active monitoring systems generate calls. Passive monitoring systems monitor existing traffic. Both methods have their own advantages. The architecture for implementation of VoIP monitoring solutions depends on the type and capabilities of the network edge infrastructure. Currently, most of the enterprise level VoIP networks have a router at the edge, performing traffic routing, firewall and network address translation functions. Some of the large enterprise level VoIP networks are equipped with special devices, called session border controllers (SBCs), performing the same functions as a router, but capable of implementing traffic forking, data/voice encryption, and quality of service. In addition, SBCs are used to hide the organisation's network topology and users from the outside IP world by screening and replacing user-specific information in all outbound packets.

Active VoIP monitoring

The diagram below illustrates an active VoIP monitoring solution architecture, with router equipment at the network edges:

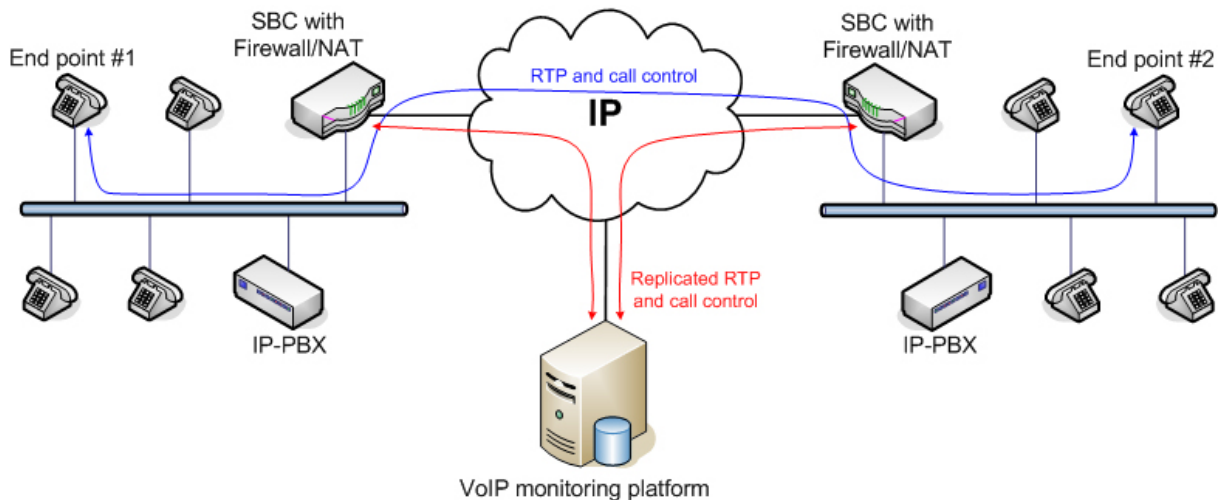


The media and call control flow, shown on the diagram above, demonstrates a call between two (could be more) end points established through Prosody S (HMP) or Prosody X. Both the media streams (RTP) and the signalling pass through the monitoring platform, and the high level control application is used to record the call and all the SIP/H.323 events and messages. Fax transactions could be recorded as well and stored as TIFF images. The system can record the RTP streams from both end points separately or together, using conferencing.

It is important to mention that the architecture of Prosody X products allows execution of the high level monitoring application on the local host or on a remote machine. Additionally, the database for monitored traffic could be on a remote server as well.

Passive VoIP monitoring

The diagram below illustrates a passive VoIP monitoring solution architecture, with SBC equipment at the network edge:



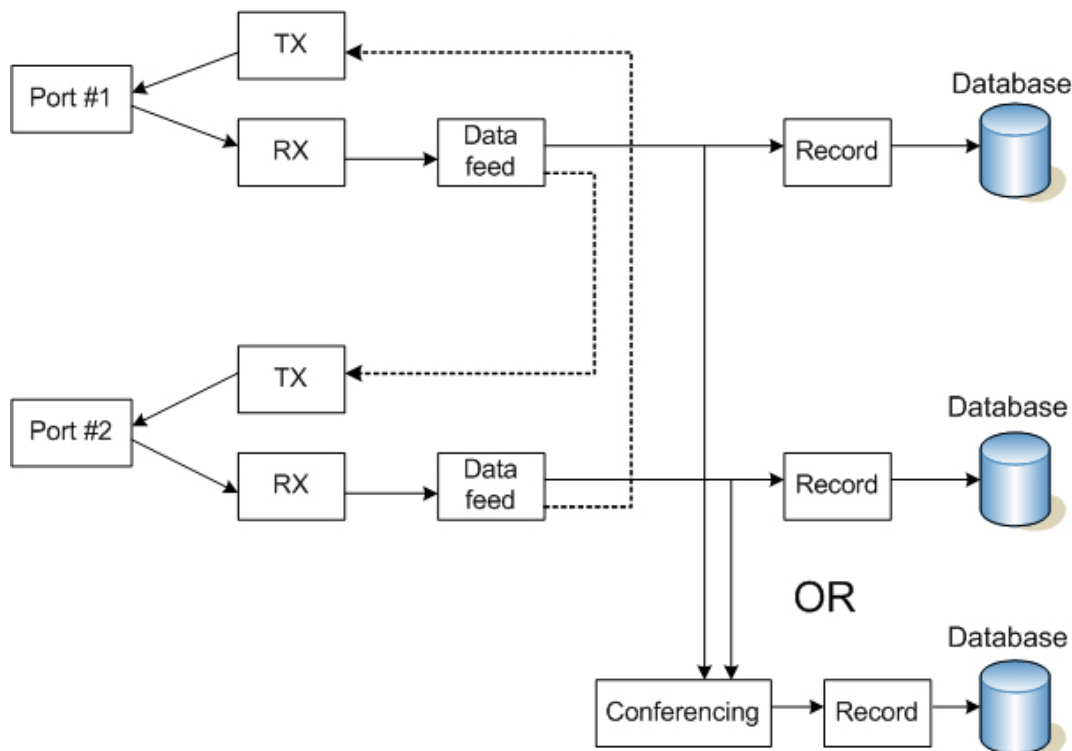
In this case, the monitoring platform, based on Prosody S or Prosody X, receives only the replicated media streams and signalling messages forked by the SBC devices. The original media and call control streams are transported inside the network, bypassing the IP passive monitoring equipment.

In some smaller enterprise VoIP networks, with no SBC equipment at the network edges, devices called network taps could be used to create permanent access ports for passive monitoring. A tap, or test access port, can be set up between any two network devices, such as switches, routers or firewalls. Taps can function as an access port for any monitoring device used to collect in-line data, including intrusion detection, protocol analysis, denial of service and remote monitoring tools. A monitoring device connected to a tap receives the same traffic as it would if it were the intended end point. The tap can send traffic data to the monitoring device by splitting or regenerating the network signal. Neither splitting nor regeneration introduce delay, or change the content or structure of information packets.

Solution design

In either of the approaches mentioned previously, the implementation of the solution requires a high level application capable of sniffing and recording all the appropriate media streams and signalling messages.

The diagram below illustrates the media flow structure, as may be implemented for either Prosody S or Prosody X media processing resources:



In the diagram above, the dashed lines connecting the data feed blocks are required for call creation and used in active VoIP monitoring solutions only.

IP passive monitoring of secure sessions

In cases when the communication between the end points is done using secure mechanisms, the possibility to implement IP passive monitoring becomes limited.

In solutions using an active VoIP monitoring approach, with Prosody S or Prosody X used for call control, the monitoring of secure VoIP sessions is possible, because the encryption key negotiation between the end users is done by the monitoring device itself.

Under the passive approach, while Prosody S or Prosody X is not involved in call control and just sniffs the network traffic forked by SBCs or network taps, the monitoring of secure VoIP sessions becomes impossible, unless explicitly authorised by SBC devices. The limitation in monitoring secure IP traffic relates to accessing to encryption keys, which are negotiated between two (or several) end points prior to call establishment. It is common that the exchange of keys for Secure RTP sessions is done using SIP under the transport layer security (TLS) protocol i.e., the keys exchange is done securely too. In that case, even if all the call control communication between the parties is monitored and recorded, the monitoring party could not obtain access to the master key necessary for decryption of the secure RTP streams.

Conclusion - monitoring the outcome

The wide adoption of VoIP platforms by enterprises imposes additional technological challenges on the organisations requiring voice networks with high levels of performance and security features. Therefore, the demand for VoIP monitoring solutions is growing fast. Voice network architectures require the creation of active and passive types of monitoring systems. Developers implementing VoIP monitoring solutions with either Prosody S or Prosody X media processing platforms from Aculab, benefit from fastest time to market and a wide set of functionality, under cost free licence, leading to flexible, scalable and cost-effective VoIP monitoring solutions.