
Enterprise Telecom Management Issues

A Corporate Whitepaper by
Kirk Vaughn,
Senior Product Manager
VoIP Technologies



Executive Summary

The migration of enterprise telephony away from the traditional Private Automatic Branch eXchange (PBX) to Voice over Internet Protocol (VoIP) is in full-swing. Whether or not a company is ready for the migration has become less relevant, as the product catalogs from the major PBX vendors are dominated by VoIP. So, the question has become when and how fast—not if the migration will occur.

VoIP is a highly disruptive technology. Its impact is felt across the organization, especially in the Telecom Management organization assigned to manage it. Not only does VoIP bring traditional PBX management issues, it adds management challenges for the data communications portion of the converged network, as well as IT security. VoIP is forcing the convergence of these three areas, imposing requirements on each for effective management and delivery of the service.

A good model to follow when preparing a VoIP migration strategy is the FCAPS model developed by the International Telecommunications Union (ITU) for managing large-scale, multi-vendor networks. The enterprise network starts to resemble a carrier network when VoIP migration starts. It encompasses equipment from multiple vendors, utilizes both Time Domain Multiplex (TDM)- and Internet Protocol (IP)-based transport networks, and effectively bridges the Public Switched Telephone Network (PSTN) and data communications network. It is easy to see why managing—and securing—this hybrid converged network has become such a challenge.

Because the network starts to resemble a small carrier network, it is natural to gravitate toward carrier-based solutions for management. Such solutions are available, but it soon becomes apparent that they are not well-suited for the converged enterprise network. Other options include legacy management systems brought over as part of the data communications or telecommunications networks. “Point Systems” are available if the inefficiency of having several independent management platforms, each serving a unique purpose, is not a concern. Yet, most point systems concentrate on one transport type or the other—they don’t manage both the TDM and IP network segments as one homogenous network. Functions such as Accounting Management, Performance Management, and Security Management become very challenging in this mixed world.

This document discusses these issues, with the intent of educating the reader on the shortcomings of today’s “point system” approach to managing a migrating hybrid network.

Table of Contents

1. Introduction
2. Legacy Voice Network
3. VoIP Network
4. FCAPS Management for the Enterprise
5. Where to turn?
6. Summary

1. Introduction

Enterprise telephony is in a transitional stage. As traditional PBX equipment is retired, or as the enterprise grows, enterprise networks are migrating to new IP-based systems. This transition is driven by heavy marketing pressure from the major voice system vendors, and by a desire to capitalize on the efficiencies of IP Telephony. The result is an enterprise network with a hybrid mix of both new and old technologies, from multiple vendors, with multiple management system components that do not integrate in a single platform.

The task of replacing traditional voice service with VoIP service is a critical one that requires careful planning and execution. But what happens after the service is installed and your trusted vendor or integration partner returns home? How does an enterprise telephony manager tackle the overwhelming task of managing the myriad details of their new hybrid network? Often, the enterprise is forced to purchase and maintain multiple management systems or rely on individual Element Managers (EM). To make things worse, most network-level management systems are designed for large-scale deployments, such as those found in a carrier-based network. Tools with an enterprise focus are scarce and lack a deep understanding of the voice application, especially when that application lives in a hybrid environment comprised of both IP and TDM transport networks.

The Migration to VoIP

Almost every enterprise telephony manager is working on a corporate strategy to address VoIP. Enterprises currently are either evaluating the technology against their future business requirements, actively testing the technology for future purchase, or already deploying VoIP in their network. VoIP is a reality, as evidenced by the amount of R&D currently under way within enterprise telephony vendors, such as Avaya and Cisco, and the large number of VoIP systems being deployed to their customer base.

The most common strategy for an enterprise VoIP deployment is to introduce VoIP in small, incremental stages. The equipment might deploy first in new office purchases or main office campuses, for an evaluation and stabilization period prior to an enterprise-wide rollout. Even once a rollout begins, an extended period referred to as the “migration period,” in which both legacy voice and VoIP systems coexist, is expected to continue for many years.

How fast can I get there?

As an enterprise migrates from traditional voice to VoIP, there are always questions as to how much of the TDM network can be replaced, and how quickly. Managing a mixed network is difficult, thus a goal of minimizing the TDM resources as much as possible, as soon as possible, is generally sought.

The reality is that TDM resources cannot be completely eliminated—even in the most aggressive “forklift” upgrades to VoIP. TDM connections are still needed to the PSTN, critical modems and fax machines need analog connections, and backup PSTN connections are needed for emergency lifeline support when primary connections go down.

Managing a suite of PBXs is challenging enough in a pure TDM environment. Eliminating the PBX and using 1FB dedicated PSTN connections to support these legacy services presents a new challenge: There are no scalable solutions to manage and control the voice application running on independent analog lines. As a result, they often go unchecked.

2. Legacy Voice Network

Management Issues

For many years, the enterprise telephony manager relied on a suite of monolithic PBX systems to deliver dialtone (with some enhanced) services to their corporate user base. These PBXs came equipped with their own element management system, sometimes integrated at the Operational Support System (OSS) or network level, sometimes not. Basic management capabilities were provided, such as Configuration Management, Call Accounting, Alarm Management, Utilization Reports, and such. But generally, these capabilities were delivered on a per-EM or per-PBX basis only; meaning that it was nearly impossible to obtain an enterprise-wide view of the network without an external correlation system to sort and consolidate the various vendor-dependent data.

Overlay systems for Enhanced Call Accounting helped solve one of the most critical issues—billing. It addressed the vital need to cross-check invoices from PSTN carriers and perform inter-company bill-back for toll charges. These third-party overlay systems collect Call Detail Record (CDR) data from each PBX and collate the data into useful reports. In many cases, a buffer box is connected to the Station Message Detail Recording (SMDR) port of each PBX for daily download to a database server for processing. This is a time-consuming and costly process—but it is effective for satisfying the Call Accounting System's primary purpose.

For performance and health/status of the PSTN trunks, expensive test equipment has been used on an as-needed basis. These systems help the telephony manager identify problems in the network, and at the very least, segment the network on each side of the PBX, the Central Office (CO) side and the station side. These test devices, when deployed on the CO side of the PBX, provide detection and visibility of line problems, frame issues, timing, alarms, and more. This visibility helps pinpoint critical issues affecting the carrier's service, or PBX line card issues requiring assistance from the PBX vendor.

Internal issues within the PBX, campus infrastructure, or handsets are analyzed by viewing data from the PBX EM. This internal infrastructure is under the control of the local PBX, and the PBX platform manages that environment quite well.

Security Issues

When establishing a VoIP network management strategy, it is important to consider all of the voice network requirements, including the need to secure legacy voice services. Misuse and abuse of the legacy voice network is often a result of improperly secured and managed network resources, as is the case with attacks on the data network through unauthorized and non-secure authorized modems on the legacy voice network, attacks against non-secure

voice systems, toll fraud, and eavesdropping. Simply securing the data network with a data firewall and Intrusion Detection System (IDS) does nothing to protect the data network or the legacy voice network from PSTN-borne attacks. Unless adequately addressed, these existing security issues from the legacy voice network will continue to impact the enterprise in a hybrid voice environment. Two of the most prominent security issues in the TDM network are the exploitation of unauthorized modems and toll fraud:

Unauthorized Modems

In a data network attack perpetrated through the legacy phone network, intruders bypass the data firewalls and IDS by using the PSTN to access unauthorized and poorly secured authorized modems (which the attacker may have identified using war dialing techniques). Attackers exploit these modems as interconnection devices between enterprise voice and data networks, and use them as an enabler for cross-network attacks.

Most unauthorized modems are non-secure and poorly configured. The focus of the employee installing them is often to gain access to the Internet for personal usage—not to maintain the security of the corporate Local Area Network (LAN). By using unauthorized modems to access the Internet, the user creates a bridge between the public untrusted network and the private trusted network, provided he has a simultaneous connection from his PC to the corporate LAN. This bypasses the IT security mechanisms in place at the data firewall and IDS. The user can upload sensitive or classified material to their Internet Service Provider (ISP), or inadvertently provide an Internet-based attacker with access to their system and the LAN beyond. A typical enterprise, even one with restricted modem usage policies and procedures, usually has some number of unauthorized and/or poorly secured modems—open “back doors” into their data network.

One case in point, a government security administrator found that unauthorized ISP access consumed 28.5% of the local access voice circuits during peak hours. In this case, unauthorized ISP access consumed almost three full T1 circuits (72 total voice channels). Security concerns aside, this is a tremendous waste of expensive voice bandwidth. Typically, voice T1 circuits cost \$1,000 per month. Elimination of this sort of unauthorized activity saved the site approximately \$36,000 per year.

Toll Fraud

It is not uncommon for after-hours employees to conduct toll fraud from unmonitored devices such as fax machines or analog devices with dedicated PSTN connections. The voice network also provides an avenue of attack against critical voice systems. Attackers can place a standard call and use Dual Tone Multi-Frequency (DTMF) tones to access and manipulate PBXs, Interactive Voice Response (IVRs), Automatic Call Distribution (ACDs), and other systems in order to commit theft of long-distance services, or create other issues. By war dialing or attacking known vulnerabilities in the voice network, attackers find lines and codes that provide a second dial tone, which they use to commit toll fraud.

In 2003, the Communications Fraud Control Association (CFCA) estimated annual telecom fraud losses worldwide to be in the range of \$35-\$40 billion U.S. dollars—up from the

previously estimated \$12 billion. The estimate was based on the results of a comprehensive opinion survey of telecom companies in 26 countries. Of the 20 to 30 different fraud types identified by the respondents, PBX/PABX/Voice Mail/CPE fraud (i.e., theft of long distance services by an unrelated third party by penetration or manipulation of Customer Premise Equipment) was ranked #2 and increasing. [1]

3. VoIP Network

Management Issues

The primary deficiency that VoIP management solutions must overcome is a lack of visibility to call flows throughout the entire life of the call. In the PBX world, visibility was never an issue. The PBX was required to maintain state, and process signaling and media for all legs of the call, for the duration of the call. Everything was routed through the PBX. This meant the PBX had access to all call statistics, measurements, and performance-related data, and could easily report on them through its EM or network management system.

With VoIP, the call control signaling and the media flow travels separately. The VoIP Call Server (IP PBX, Softswitch, Call Manager, Gatekeeper, etc.) has a reduced role in the setup of VoIP calls. The call server is responsible for authenticating a session, locating the endpoints, negotiating the setup between endpoints, and ensuring that

each endpoint has the proper information to establish a Real-time Transport Protocol (RTP) media session. Once it has fulfilled those duties, it steps back and waits for a new request such as a call hang-up before becoming involved again. The media flows are allowed to take the path of least

resistance through the network. This means that the call server knows what happens at the beginning of the call, and what happens at the end of the call, but rarely does it know what happens in between (unless some supplementary services are used, such as call transfer or call hold, in which case the call server helps deliver those services).

The media gateway assists with the call server's lack of visibility by collecting statistics for signaling and media destined for the PSTN. This is considered a critical boundary, and as such, the media gateway is asked to collect statistics and delivery information on each call and report them back to the call server and management system.

Figure 1 illustrates the contribution performed by the media gateway, providing both media and signaling statistics and other information to the call server and management system.

The real "blind spots" in managing the network lie in the campus-level station-to-station traffic and traffic traversing a Wide Area Network (WAN) boundary or IP trunk. In these

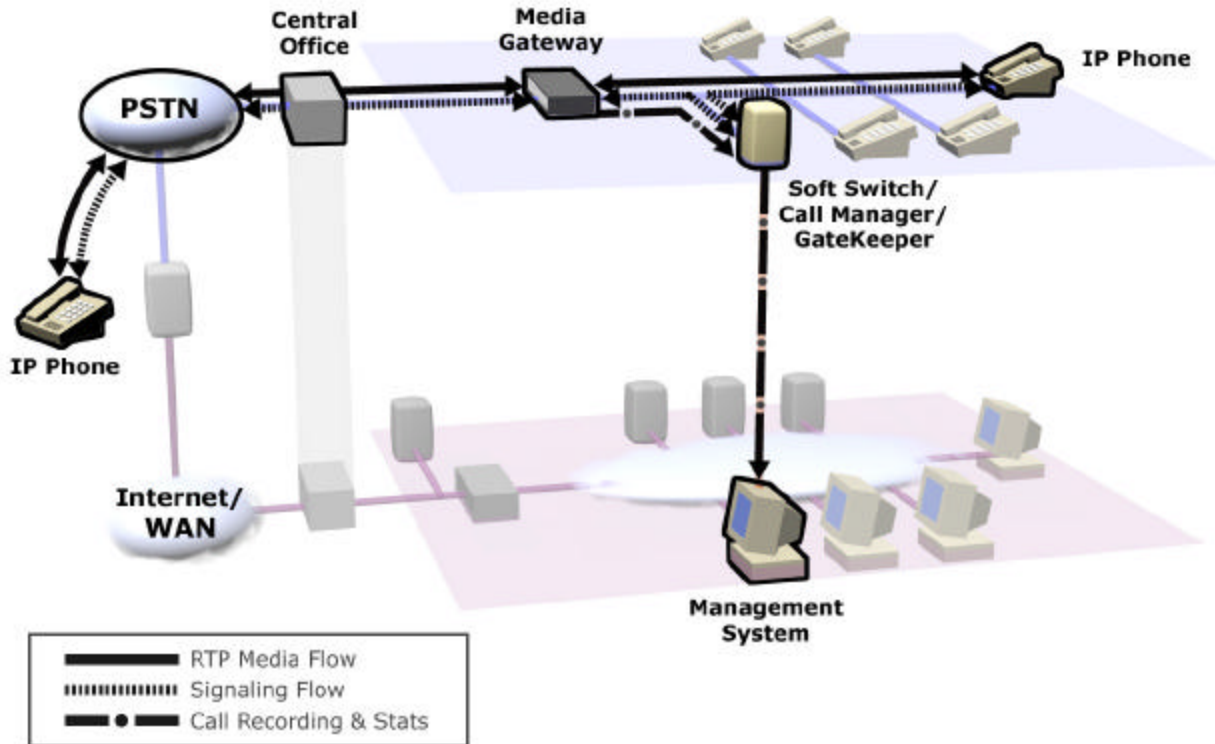


Figure 1 – Media Gateway in an IP Network

scenarios, the call server must rely on additional management nodes distributed throughout the network to provide needed visibility. Media characteristics such as performance and Quality of Service (QoS) measurements, data packet integrity, and delivery precision must be gauged by a separate system capable of measuring these flows. Signaling is often analyzed for security purposes by adjunct security appliances responsible for things such as Network Address Translation (NAT), protocol integrity, and anomalous activity. Call accounting is enhanced by appliances that see the signaling flows at various parts of the network, including across the PSTN, and that can correlate all of the data into one single CDR.

Security Issues

Security must be a key requirement for any VoIP network management strategy, because a successful VoIP deployment hinges on the strength of its security. If the VoIP network is not secure, the expected levels of quality and reliability cannot be maintained. VoIP networks and network protocols have inherent vulnerabilities that expose the enterprise to legacy threats present on the traditional voice network, such as toll fraud and eavesdropping. They also introduce new threats, such as attacks on Call Servers, Denial of Service (DoS) on signaling and media, DoS on gateways and legacy voice systems, protocol attacks, QoS theft, and attacks against IP phones. Traditional data security solutions are not designed to handle VoIP's unique real-time and reliability requirements, nor are they designed to perform the application-level inspections required to prevent many of these attacks. By failing to monitor VoIP traffic at the application level, traditional data security solutions leave a security gap through which Call Servers, IP phones, and other components are exposed to attack. Unless adequately addressed, these security issues can cripple a VoIP network:

Attacks Against Call Servers

The most critical vulnerabilities are those present on Call Servers, the heart of any VoIP network and the primary target for attackers. Call Server vulnerabilities include their operating system and the Call Server's supporting services (e.g., web server or database), both of which are non-secure and carry well-known vulnerabilities. Vulnerabilities also exist in the voice applications, which can be exploited to create a DoS condition, provide unauthorized access, or perform unauthorized actions such as terminating a call, allowing a toll call, or impacting a user's phone services.

Protocol Attacks

Session Initiation Protocol (SIP) is considered the future protocol for VoIP. However, most SIP development has focused on feature sets and interoperability, with limited attention paid to security. Inherent SIP/VoIP vulnerabilities present for the majority of vendor implementations include registration hijacking, proxy impersonation, SIP message tampering, session tear down, and DoS.

Registration Hijacking

Registration hijacking occurs when an attacker impersonates a valid User Agent (UA) to a registration server, and then registers itself, causing all requests

intended for the legitimate UA to be directed to the attacker instead. Registration hijacking can result in toll fraud, automated attacks to generate many calls resulting in excessive toll charges or a DoS condition against a gateway or PBX. Attackers can also redirect all incoming (phone) or outgoing (gateway) calls via their UA to eavesdrop or monitor calls.

Proxy Impersonation

A phone or proxy server can be tricked into communicating with a rogue proxy server. Proxy impersonation can occur through packet interception, domain registration hijacking, and DNS impersonation, allowing an attacker to eavesdrop, track, redirect, and block calls, or perform selective and wholesale DoS.

Message Tampering

Message tampering occurs when an attacker intercepts and modifies packets between proxies. By modifying packets, attackers can redirect all incoming calls via their UAs to eavesdrop on the calls. Attackers can also block calls or send unexpected calls through media gateways, which can tie up TDM trunking or switches.

DoS Attacks

Denial of service occurs when an attacker sends a single, well-crafted packet to the target system, causing it to fail, resulting in a loss of function for a Call Server or other VoIP components. DoS also occurs when an attacker causes a flood of packets to be sent, overwhelming the target and preventing it from handling legitimate requests. DoS against a SIP system can occur through registration hijacking, proxy impersonation, session tear down, message tampering, or other means not described here.

The 2003 CSI/FBI Computer Crime and Security Survey reported that DoS had risen to be the second most expensive computer crime among survey respondents. [2] In the 2004 survey, DoS emerged as the most expensive computer crime (replacing theft of proprietary information, which had been the leading loss for 5 consecutive years). The combined DoS losses for both years exceeded \$91 million. [3] Considering the currently small percentage of VoIP deployments, DoS attacks against VoIP systems cannot yet be a significant contributor to these statistics. However, considering DoS against a SIP system is simpler to achieve than DoS against other data systems (due to VoIP's QoS requirements), the 2003 and 2004 surveys paint an ominous picture of future DoS attacks on non-secure voice services.

Attacks Against IP Phone/Soft Phone

Many IP Phones and softphones are vulnerable to unauthorized remote access and unauthorized local access. Virtually all IP phones are programmable and can be upgraded with new firmware, so an authenticated user can transfer, block, forward calls, etc. Additionally, an attacker with local access can install a hub between the IP Phone and the switch and eavesdrop on packets. For many IP Phones, an authenticated user can change settings to create a DoS condition for the IP Phone, which if exploited for hundreds or thousands of phones within an enterprise, would require a great deal of effort to recover.

4. FCAPS Management for the Enterprise

It is obvious that there are many issues facing the enterprise telephony manager, regardless of whether the network is legacy voice, VoIP, or a hybrid mixture of both. The FCAPS management model is a useful tool for the telephony manager defining the requirements and boundaries of a comprehensive management and security solution. The FCAPS management model was standardized by the International Standard's Organization (ISO), and consists of network management concepts developed by the ITU for managing large-scale telephony networks. With adaptation to the unique requirements of the enterprise, the FCAPS model is very applicable to an enterprise data or VoIP environment. FCAPS categorizes the wide array of management systems and information into five discrete management categories: Fault, Configuration, Accounting, Performance, and Security management.

Table 1 illustrates some of the common TASKS associated with each of the five FCAPS categories. These categories provide the needed functionality to effectively manage all aspects of the enterprise telephony network.

Fault Management consists of monitoring and collecting data on network problems (i.e., faults), such as alarm status, and applying intelligent analysis techniques to the collected data for proper action. For example, dropped packets or occasional network bottlenecks are common and may only require event logging. However, alarms that are classified as severe (red) or warning (yellow) may signal that other problems are imminent and require immediate response. A consolidated alarm management system is capable of collecting the various alarm information from multiple sources (including EMs, performance managers, and security systems), and presenting the alarm data in a consolidated and managed fashion.

Configuration Management includes identifying and tracking network resources and resource details. The information is often stored as managed objects in directories or databases for easy retrieval and

management. Configuration management allows for orderly activation/deactivation of certain resources, and provides a change management process for tracking changes to the network, including software revisions.

Accounting Management involves collecting and tracking network resource usage metrics and reporting utilization costs to the appropriate parties. Accounting Management Systems (i.e., billing systems) should have the capability to not only track high-cost resources (e.g., long distance, international, and 900 toll numbers), but also to report, and track enterprise and departmental usage of the resources. Additionally, usage and cost reporting needs to be consolidated from across the entire voice network, independent of vendor or implementation—not segmented between the legacy PBX and VoIP networks.

Performance Management comprises gathering and analyzing critical end-to-end network performance metrics under both normal and degraded conditions. This includes collecting statistical data from both within the network protocols (i.e., RTCP or D-channel analysis), and by actively monitoring the traffic. Active monitoring techniques include real-time analysis on a channel or packet basis, or using synthetic transactions to monitor network capabilities and performance. Performance Management also includes setting thresholds and providing reports and alerts to other systems, such as sending SNMP traps to the alarm manager, when network performance degrades below acceptable levels.

Security Management entails minimizing and attempting to eliminate unauthorized access to the voice and data network through vulnerabilities in the traditional voice and VoIP networks. It involves monitoring and controlling access to specific network resources and applications, ensuring access is limited to only legitimate use by authorized internal and external users, providing controlled access to key resources, and providing notifications (alarms) when breach attempts occur. Security Management also includes implementing prescribed corrective actions when violations of established security policy occur, such as termination of active phone calls or denial of access to phone calls in violation of policy.

FCAPS MANAGEMENT TASKS				
Fault Management	Configuration Management	Accounting Management	Performance Management	Security Management
Alarm monitoring, collection and analysis	System turn-up	Service usage tracking and reporting	Data collection	Network Edge (NE) access control
Trouble detection	Network provisioning	Services billing	Report generation	NE function enabling
Trouble correction	Autodiscovery		Data analysis	Access logging
Test and acceptance	Back up and restoration			User-level access monitoring
Network recovery	Database handling			

Table 1 – FCAPS Functionality

5. Where to Turn?

A properly designed enterprise management system should address issues that cross boundaries between the traditional voice network and the VoIP network. For instance, the following legacy management activities continue in a hybrid VoIP/TDM environment:

- Collection and analysis of call detail and billing records
- Real-time monitoring and control of call activity to/from specific destinations
- Real-time monitoring of health, status, and availability of resources and equipment (e.g., T1, 1FB, PBX alarms)
- Collection, analysis, and reporting on resource utilization

The ideal solution is an enterprise-focused system with both management and security applications on a single platform. The solution should cover the entire integrated network, regardless of whether an enterprise is dealing with a traditional voice network, a VoIP network, or a hybrid mixture of both. FCAPS is a good tool for evaluating an enterprise's needs, but it is unrealistic to imagine that a security and management tool for the voice network could replace the Fault Management system (such as HPOpenview® or Tivoli®) that is generally already in place for fault management of the enterprise data and telephony network. It is also unrealistic to expect that a third party system could perform the configuration management duties needed for the VoIP infrastructure better than the element management system specifically designed by the vendor.

Figure 2 illustrates contributions that could be provided by a hybrid network management system.

However, the remainder of the FCAPS model is certainly in need of additional support and is best addressed by an integrated, vendor-neutral, transport-neutral management system. This system should address the Accounting Management needs by providing cross-vendor reporting in a hybrid environment, correlating calls across both the PSTN and IP network, and storing call records as a single instance rather than one for the IP portion and another for the TDM portion of the call.

The solution should address Performance Management by measuring the performance of the voice application not only from end-to-end, but at key points within the network as well. Additionally, it is not sufficient to look only at

network performance. Network performance tools are valuable when performing root-cause analysis on a problem. Often, a better measurement is needed for the application itself, which might include factors related to application signaling performance, codec performance, and a human-perception factor to account for a user's perception of the quality of the call. A snapshot measurement on a per-call basis is useful for trend analysis and identifying deteriorating network conditions, which can be analyzed using the root-cause analysis network toolset, when needed.

A complete solution for applying FCAPS methodology to managing the enterprise must include management and enforcement of security policy and techniques. Security breaches can directly affect the performance of a network and its applications, thus it is imperative to include security in the overall health assessment of the network. Security-focused solutions should include application-layer security capabilities to prevent the types of attacks discussed previously. They should also include a policy-based capability to monitor authorized user activity on the network, which will help prevent misuse of network resources and reduce exposure of the data network to unapproved ISP activity.

6. Summary

The reality for enterprise communications is that legacy voice networks are needed, and will remain for a long time, despite all the hype surrounding the benefits of an "all VoIP" world. Logically, the legacy voice network and the VoIP network need to be combined and managed as a homogenous hybrid network. The tools to manage this hybrid network are available, but they generally come packaged in expensive purpose-built wrappings. Large enterprises have the most flexibility in terms of resources and budget for installing these purpose-built management systems, but even they must take a step back and decide if this is the right approach. What is needed is an appropriately scaled, yet integrated system that addresses the FCAPS model for providing end-to-end multi-vendor management and security of the inevitably hybrid voice infrastructure. The security and management of the hybrid network is an important aspect of a VoIP migration strategy, and a system that uses an integrated, scalable approach to addressing the security and management issues should be considered.

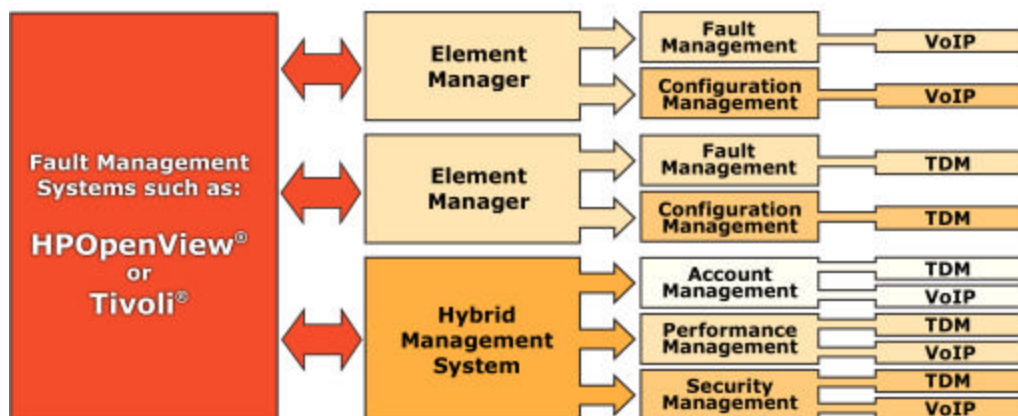


Figure 2 – Enhanced Hybrid Management System Structure

Acronyms

1FB – One Flat Business rate
ACD – Automatic Call Distribution
CDR – Call Detail Record
CO – Central Office (carrier or telephony provider)
CPE – Customer Premise Equipment
DoS – Denial of Service
DTMF – Dual Tone Multi-Frequency
EM – Element Manager
FCAPS – Fault, Configuration, Accounting, Performance, Security management
IDS – Intrusion Detection System
IP – Internet Protocol
ISO – International Standard's Organization
ISP – Internet Service Provider
ITU – International Telecommunications Union
IVR – Interactive Voice Response
LAN – Local Area Network
NAT – Network Address Translation
NE – Network Edge
OSS – Operational Support System
PABX – Private Automatic Branch eXchange
PBX – Private Branch eXchange
PSTN – Public Switched Telephone Network
QoS – Quality of Service
RTCP – Real Time Control Protocol
RTP – Real-time Transport Protocol
SIP – Session Initiation Protocol
SMDR – Station Message Detail Recording
SNMP – Simple Network Management Protocol
TDM – Time Domain Multiplex
UA – User Agent
VoIP – Voice over Internet Protocol
WAN – Wide Area Network

References

- [1] Communications Fraud Control Association (CFCA), *Background and additional information for news writers and editors considering writing a story on CFCA's recent telecom fraud survey*. March 14, 2003.
http://www.cfca.org/Documents/fraudloss_background.pdf
- [2] Computer Security Institute, *2003 CSI/FBI Computer Crime and Security Survey*. 2003.
http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf
- [3] Computer Security Institute, *2004 CSI/FBI Computer Crime and Security Survey*. 2004.
http://i.cmpnet.com/qocsi/db_area/pdfs/fbi/FBI2004.pdf

SecureLogix, SecureLogix Corporation, and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2004 SecureLogix Corporation. All Rights Reserved.



13750 San Pedro, Suite 230 • San Antonio, Texas 78232 • PH: 210.402.9669 • FX: 210.402.6996 • TF: 800.817.4837
www.securelogix.com
