

CASE STUDY: A Leading Service Provider Improves VoIP Robustness, Availability and Security via Service Assurance

The Service Availability Challenge

Service availability is of paramount importance to any provider of real-time services, like Voice over IP (VoIP). One major U.S.-based service provider understands firsthand that the ability to test product robustness, availability and security (RAS) has a direct, measurable impact on the bottom line. This Tier-1 provider offers quad-play services – voice, video, data and wireless -- and serves customers in both the business and consumer markets.

This provider knows that its ability to maintain its edge in these highly competitive businesses hinges on the ability to rapidly develop and deploy innovative revenue-generating services, including hosted VoIP, real-time conferencing, streaming media and other interactive services. But as it pleases customers with hot new services, it must still meet or exceed industry-standard expectations for stability, reliability and availability: 99.999% uptime.

High Cost of Downtime

Achieving the service levels that customers expect means minimizing downtime. There are two types of network downtime:

1. Degradation, when a service is slower than usual, perhaps to the point of being useless, and
2. Outright outage, when a service is unavailable.

The second is usually more serious than the first, but not always. For example, a VoIP phone user may become so frustrated at an unreliable service that s/he leaves in a huff and never returns. This is indeed a loss for the service provider that provides the VoIP service directly or indirectly to this user.

Like other real-time services, downtime in VoIP services incurs several significant costs for a service provider. These costs include:

- lost revenue,
- customer churn,
- avoidable support costs,
- decreased average revenue per user (ARPU).

This leading provider estimates that the average hourly downtime cost is over \$130K, and the **average annual downtime cost is \$23.4M**, sometimes higher than \$100M. It's imperative for this provider to minimize system downtime to avoid customer churn, which improves its bottom line, and maximizes the return on the ever-increasing customer acquisition cost.



CHALLENGE

- Rapidly roll out innovative, revenue-generating VoIP services while ensuring that those services meet the expected service availability and reliability levels;
- Prevent costly service outages and degradation, and reduce customer churn and subscriber support costs;
- Identify potential sources of service quality issues before they impact the customer experience or VoIP infrastructure performance.

SOLUTION

Mu-4000 Analyzer

RESULTS

- Improved service availability for VoIP and unified-communication services, establishing processes to maximize uptime of additional services such as video streaming;
- Reduced customer churn and improved bottom line as a result of significantly improved VoIP service quality;
- Identified a zero-day vulnerability in a session border controller, which was patched prior to service rollout;
- Automated and conducted comprehensive testing of vendor products more efficiently, and streamlined problem resolution process with vendors.

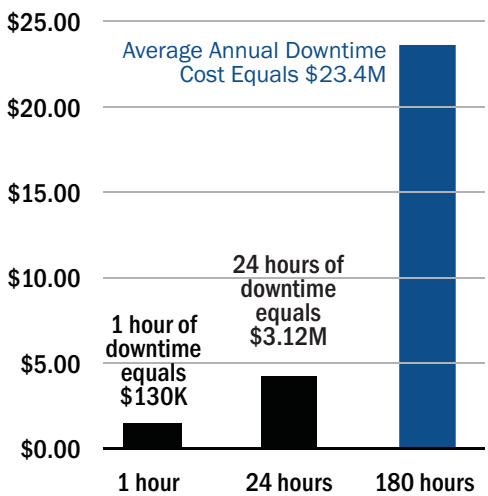


Figure 1. Average Downtime Cost in Millions

Difficulties in Testing VoIP Deployments

Due to these high costs, service providers are quite motivated to reduce network downtime and maintain high service quality. However, achieving this goal in VoIP-based IP communications solutions is a daunting task. VoIP-based networks depend on many hardware and software components and middleware, and each device is itself a complex hardware/software system on its own. As the system complexity increases, implementation mistakes become ever more likely. These device flaws create opportunities for vulnerabilities in VoIP systems, which can degrade service and lead to downtime.

Until now, service providers have not had effective tools to systematically address the root cause of system robustness issues. Existing system testing tools have several major limitations:

- **Depth:** not able to find significant percentage of bugs or vulnerabilities in systems;
- **Agility:** not able to keep up with the pace of product development and deployment;
- **Breadth:** not able to provide thorough coverage.

Improving VoIP Service Quality with Mu

This leading service provider has turned to Mu's service assurance solution, which is now an integral part of the provider's world-class testing and certification lab. Service assurance helps determine how vendors' products will meet its standards for robustness so the service provider knows in advance whether the products will survive in the real-world production network environment.

With the Mu solution, the provider's architects define purchasing acceptance criteria, so robustness is "designed-in" from the start and baked-in throughout the entire deployment life cycle. Its engineers use the Mu solution to test products throughout the life cycle to proactively identify and address robustness issues that may have caused downtime in a production system. This allows the service provider to take actionable steps toward remediation, before vulnerabilities impact the reliability and security of its VoIP services.

Figure 2 is a simplified network diagram of this service provider's VoIP architecture. Table 1 summarizes the network elements that the Mu solution analyzes and the benefits for the service providers. Please refer to the "Use Case Details" section for more information.

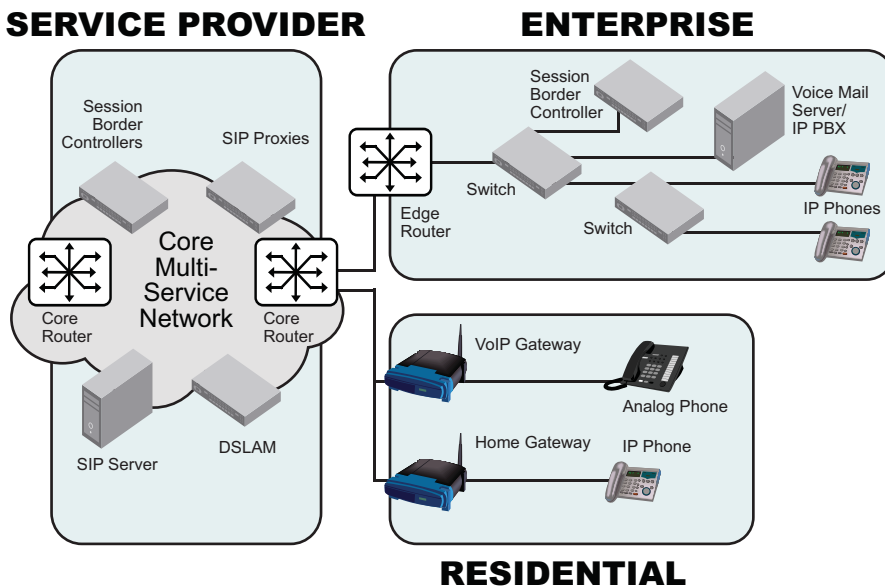


Figure 2. Simplified VoIP Network Architecture Diagram

Business Benefits from Using Mu

After using Mu's service assurance solution for a year, this provider has achieved significant business benefits. With comprehensive security and robustness testing incorporated into its entire service life cycle, the provider has improved its VoIP service uptime, and has thereby avoided service disruptions that would have otherwise impacted revenues, customer retention rate and overall customer satisfaction.

Key results include:

- Reported a significant reduction in customer churn and SLA penalties as results of improved service availability and quality.
- Uncovered a serious flaw in a session border controller prior to deployment, and thus avoided a service outage.

- Reduced costs in several areas thanks to the proactive approach to problem resolution.

Reducing Total Cost of Ownership (TCO)

Lower total costs contribute to a faster and higher return on investment (ROI) for IP networks. The following are three major cost categories that are key drivers in lowering TCO:

- CapEx,
- OpEx,
- Opportunity costs.

Reducing CapEx

Mu helps this service provider ensure the VoIP devices and applications it purchases are robust, which prevents wasting CapEx on low quality products. Mu provides an integrated analysis approach, so this service provider does not need to buy numerous point solutions that provide only a subset of the analysis capabilities of Mu. Therefore, the provider saves on equipment outlay. Furthermore, Mu's solution platform can be seamlessly integrated with other already-purchased testing tools and homegrown solutions, so that existing capital investments are fully preserved and leveraged.

Reducing OpEx

Mu's solution has helped the service provider to reduce their operating expenses in the following areas:

Layer	Network Elements	Mu Tested	Benefits from Using Mu
Backbone	Router	☑	<ul style="list-style-type: none"> • Harden VoIP infrastructures • Reduce TCO by addressing product vulnerabilities early
	SIP Proxy	☑	
	Firewall	☑	
	IPS/UTM	☑	
Core Services	Core Router	☑	<ul style="list-style-type: none"> • Robust digital dial-tone • Improve audio clarity
	SIP Server	☑	
	Session Border Controller	☑	
	SIP and IMS Endpoints	☑	
	Digital Subscriber Line Access Multiplexer (DSLAM)	☑	
Customer Premises Equipment (CPE)	<i>Enterprise</i>		<ul style="list-style-type: none"> • Minimize voice quality issues such as packet loss, delay, echo, etc. • Characterize system responsiveness to identify problem spots • Secure triple-play control planes
	Switch	☑	
	Edge Router	☑	
	Session Border Controller	☑	
	IP PBX	☑	
	IP Phone	☑	
	<i>Residential</i>		
	VoIP Gateway	☑	
	Home Gateway	☑	
	IP Phone	☑	

Table 1. Comprehensive Testing for VoIP Services

WHERE	HOW
Customer Acquisition Costs	Because customer churn was reduced, the service provider not only improved their bottom line, but also maximized its return on the ever-rising customer acquisition cost.
Avoidable Support Costs (Incident Response)	Mu finds bugs before service rollout and upgrade, so the frequency and severity of downtime has gone down. Therefore, support staff need not spend as much time on resolving downtime-related customer issues.
SLA Penalties	Due to significantly improved service quality and customer satisfaction level, the service provider has reduced cost in SLA-related penalties.
Vendor Problem Resolution	Because of Mu's full range of remediation tools, interactive charts and detailed reports, resolving issues with vendors has become easier and less time-consuming.
System Upgrades & Patches	Mu's regression testing feature enables its testing staff to accurately verify bug fixes from vendors.
Ongoing Operation	Mu's run-to-completion analysis capability does not require human intervention once started, and automatically pinpoints flaws.
Staff Training and Retention	Mu's analysis templates help disseminate scarce security knowledge, and establish service assurance best practices across the entire organization. The provider finds it easier to train new analysts and provide professional development in service assurance for existing staff.

Reducing Opportunity Costs

Opportunity costs, though difficult to measure, are very real. After deploying Mu's solution, this service provider has significantly reduced its opportunities costs. These costs represent lost opportunity for profit resulting from network downtime, inability to deploy new service quickly, application or device failure, etc.

Use Case Details

Thorough Attack Surface Coverage

With the Mu-4000, the service provider is able to methodically identify areas of product weakness that might undermine the service provider's business operations. The service provider's testing team feels that the Mu-4000 provides the only way to get deep, comprehensive attack surface coverage of the protocol implementations across its VoIP system.

The service provider uses the Mu-4000's Dynamic Stateful Fuzzing engine to thoroughly exercise the multi-packet exchanges among complex protocols in all valid and invalid states. VoIP uses the Session Initiation Protocol (SIP) to control communications. Furthermore, SIP leverages many of the mechanisms developed for the HTTP and SMTP/MIME protocols, thus inheriting weaknesses and vulnerabilities. The service provider is painfully aware that SIP is known to have a large number of semi-interoperable implementations and many extensions, which makes it challenging for network equipment manufacturers to ensure robustness and interoperability, especially in multi-vendor deployments as would be found in any real network.

Comprehensive Support for Analyzing VoIP Deployments

With the Mu-4000, engineers at this service provider test millions of unique scenarios and gain better visibility into issues that would affect service availability. For VoIP implementations, the Mu-4000 supports:

- H.323/H225.0/H.245 call signaling,
- SIP (including IMS endpoint functionality),
- MGCP (including NCS profile),
- H.248/Megaco (IMS profile),
- RTP/RTCP, and
- deeply stateful attacks for several dozens other protocols that are necessary for VoIP.

Attacks are delivered over any valid transport, using any valid or appropriate authentication mechanism for the protocol in question.

For example, when testing session border controllers, the engineers at this Tier-1 operator use the Mu-4000 to analyze the SIP implementation on the operational port as well as management protocols including HTTP, SSH, Telnet and FTP. They use similar test methodology across other integral elements of the VoIP infrastructure, including SIP/IMS endpoints, call managers and proxy servers.

In fact, security engineers using the Mu-4000 **uncovered a serious flaw in a session border controller** just prior to deployment. This flaw, in a production network, would have caused service degradation and security issues. With the Mu-4000, the engineers had the benefit of detailed documentation about the vulnerability, which it provided to the vendor to accelerate the remediation process.

Automation Improves Efficiency

With the Mu-4000, engineers cover more test scenarios than would be humanly possible with scripting or manual efforts. They also use the Mu-4000 appliance to automate other toolsets, including the open-source vulnerability analysis tool Nessus. A time-saver is the ability to automatically re-run any test with one-touch regression testing, which allows them to validate that a vendor's patch truly fixes the issue. Another key feature the engineers enjoy is automatic fault isolation. The Mu-4000 continuously manages the analysis process without human intervention, creating checkpoints and isolating faults as they are discovered via the chosen monitor (serial console, syslog, ssh or telnet).

The service provider is also starting to leverage the new DoS module from the Mu-4000. This module enables automatic modeling of stateless traffic – identical to the traffic found in denial-of-service traffic targeted both at the network products and application services. The certification and testing lab is eager to use the DoS module to gain insights into two aspects of the system in a controlled environment – availability during the attack and graceful recovery after the completion of the attack.

Ease of Use

The testing team also appreciates Mu-4000's GUI for ease of use. As a Web-based appliance, the Mu-4000 is easy to install and is intuitive to use. Wizards and templates guide the engineers through the analysis process. Creating and using a template is a simple process that allows the engineers to define attack types, monitor channels and to specify action(s) to be taken in response to events. Test-center staff simply selects any of the Mu's protocols and then configures the comprehensive variety of custom attack parameters in each template. The XML-based templates are also portable using the Mu-4000 for any aspect of the analysis.

Templates further a "Best Practice" approach that is easily shared organization-wide and with the engineers that have complementary skill sets.

Ongoing Service Assurance

By verifying that vulnerable VoIP products are not deployed into production, this Tier-1 service provider avoids most significant problems down the road, including service degradations and downtime. The Mu-4000 is finding its way across the entire deployment lifecycle from the initial product purchase to subsequent upgrades. The service provider began using the Mu for acceptance testing, but now uses it for verification testing of every code revision and application level change.



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317

CASE STUDY: Service Provider Tunes in IPTV Service Reliability and Security with Thorough Security Analysis

The stakes are nothing less than the future of entertainment and communications. It is a battle to be the company that brings video, voice and data services to homes and businesses in the United States and across the world. Telecom, ISP, cable and satellite companies are competing fiercely to earn their share of Internet Protocol Television (IPTV) revenue.

An estimated 55 million people will subscribe to IPTV services by 2010, according to the Open IPTV Forum. But before any service provider can tap into new revenue streams from IPTV service delivery, it must make a massive investment necessary to build a robust, secure digital TV infrastructure.

A leading service provider is piloting IPTV service to consumers in several communities in the United States. For this Tier 1 telecom service provider, delivering high quality IPTV will generate new revenues that will offset declining voice revenues. IPTV will enable the company to more effectively compete with the cable industry's successful triple-play services. It also hopes that IPTV will help it create long lasting customer relationships, which will ameliorate the industry's pervasive issues with customer churn.

Seizing the IPTV Opportunity

To achieve this promising future, the Chief Architect of IPTV at this service provider is overseeing a massive overhaul of its network architecture. IPTV is predicated on an intelligent, next-generation network infrastructure with advanced security that can deliver IP-based broadcast and video-on-demand (VoD) as well as other rich content. 2008 is a promising year for IPTV, given the early popularity of the service among elite users. The service provider hopes to capitalize on events such as the Beijing Olympics, which are ideal for IPTV, and spread the demand for IPTV among the broader population.

The service provider delivers broadcast TV as well as video-on-demand today in its IPTV pilot in several communities in the United States. Subscribers can order content on demand, so they can choose entertainment they want to watch when they want to watch it. The service provider plans to add the ability to interact with scheduled programs, such as the ability for viewers to vote with their remote controls.

Based on the success of on-demand ad delivery on Internet sites, the service provider has high hopes that targeted customized advertising can be a significant revenue stream. By delivering more relevant advertising to consumers, the service provider can charge advertisers a premium.



CHALLENGE

- Offer broadcast TV, video-on-demand, interactive TV and targeted advertising to consumers as part of an IPTV pilot, which will generate new revenue streams and offset declining voice revenues;
- Compete more effectively against triple-play services from cable companies;
- Identify potential sources of service degradations before they impact the customer experience and service level agreements;
- Ensure that IP-based video can share the next-generation network without impacting the availability of other revenue-generating subscriber services, including VoIP;
- Verify that IPTV network equipment is free from zero-day and known vulnerabilities.

SOLUTION

Mu-4000 Analyzer

RESULTS

- Successfully piloted IPTV services to consumers in several regions in the United States, paving the way for future rich content service rollouts;
- Met massively high service availability requirements for IPTV without impacting VoIP and other services that run on the same next-generation network infrastructure;
- Verify that IPTV products are free from vulnerabilities that may affect security or robustness before products are purchased and deployed into the production network;
- Automate and conduct comprehensive testing of highly complex IPTV applications and equipment to meet aggressive service rollout schedule.

The service provider has aggressive plans for other IPTV services. Integration with other communication services, such as phone or the PC, will allow subscribers to interact with friends and other people while watching TV. With presence and text messaging, subscribers can see which of their friends are online and chat about the show they are watching. Users can receive on-screen notifications about incoming calls or requests for video chat. Integration with mobile devices means that subscribers can download content to their mobile devices. A parent away from home can use a mobile phone to approve and unlock pay-per-view content that the children ordered.

The High Cost of Downtime for IPTV

Any market shift creates the potential of huge rewards and risks, and IPTV is no different. This service provider's IPTV pilot is backed by the build-out of a next-generation network architecture that can scale to handle the massive quality of service and availability demands of digital TV. Although this is a pilot, consumers will nevertheless expect that their IPTV service will "just work" -- without hiccups or hitches.

To meet those expectations, the service provider must proactively plan to deal with service degradations as well as service outages. Poor video quality or repeated outages for video services, especially for broadcast, will no doubt result in dissatisfied customers and customer turnover. It will also increase customer and network support costs, which is particularly concerning given the massive investment required to build the IPTV infrastructure. Negative customer feedback and bad press associated with a failed pilot puts future revenue streams at risk and could damage the company's brand.

IP network video is inherently intolerant of packet loss. IP network video is highly compressed and the video codecs don't recover from packet loss at the network layer, which means that losing a single packet of IP-encapsulated video can result in visibly degraded video quality. The quality of service challenge is compounded when considering that IP video will run on the same network with VoIP, best-effort Internet traffic and over-the-top video. Availability of these other subscriber services may be impacted by the robustness and security of IPTV services.

The service provider must also protect the IP infrastructure that carries the video signals. It has seen some of its Tier 2 competitors roll out IPTV services without the necessary attention and been hit by cyber-attacks and industry backlash. As a Tier 1 provider, a poorly planned rollout could cause long-lasting damage to the company's brand.

IPTV is subject to the same hacker attacks, threats and vulnerabilities that plague other network-based services such as the Internet. Attackers are often quick to exploit services in their early phases of adoption on the assumption that the service is not fully hardened.

Denial-of-service (DoS) attacks are of particular concern for IPTV. The nature of direct subscriber interaction makes the video serving infrastructure more susceptible to attacks. Video servers must be highly protected, as they are vulnerable to DoS, TCP and application-level attacks. Even if a DoS attack doesn't cause a service outage, network performance may degrade, which can impact video quality. Many other IPTV infrastructure elements and application services are at risk. For instance, an attack on a server that handles channel switching may overload that server and leave consumers without the ability to change the channel with their remotes.

Another risk is the subscriber's home network itself. IPTV may be carried over a subscriber's home network, along with Internet traffic, gaming sessions, and VoIP calls. A security breach on one of the subscribers' computers may open up the opportunity for attacks on the service provider's IPTV infrastructure, which also creates risk. The service provider must be assured that set-top boxes and other home equipment are free from vulnerabilities and security weaknesses.

Protecting IPTV Robustness and Security with Mu

Ensuring the robustness and security of the IPTV infrastructure is a multi-faceted undertaking, requiring the protection of the video serving infrastructure as well as the network infrastructure. Success was predicated on building IPTV system that can deliver high quality services and survive attacks. Given the unprecedented complexity and the aggressive rollout schedule, the Chief Architect knew he needed find efficiencies to accelerate the process of assuring that the IPTV elements will meet the company's standards for robustness and security.

The Chief Architect turned to Mu's security analysis solution for comprehensive security and robustness testing. With Mu analyzer, the engineering team test IPTV video serving and network infrastructure equipment for known and zero-day vulnerabilities prior to purchase and deployment into the network. With Mu, engineers validate the network's ability to defend itself against attacks and verify the performance of IPTV services when under attack, thus minimizing the risk of service degradation and outage. Refer to the "Technical Details" section for more information about use cases.

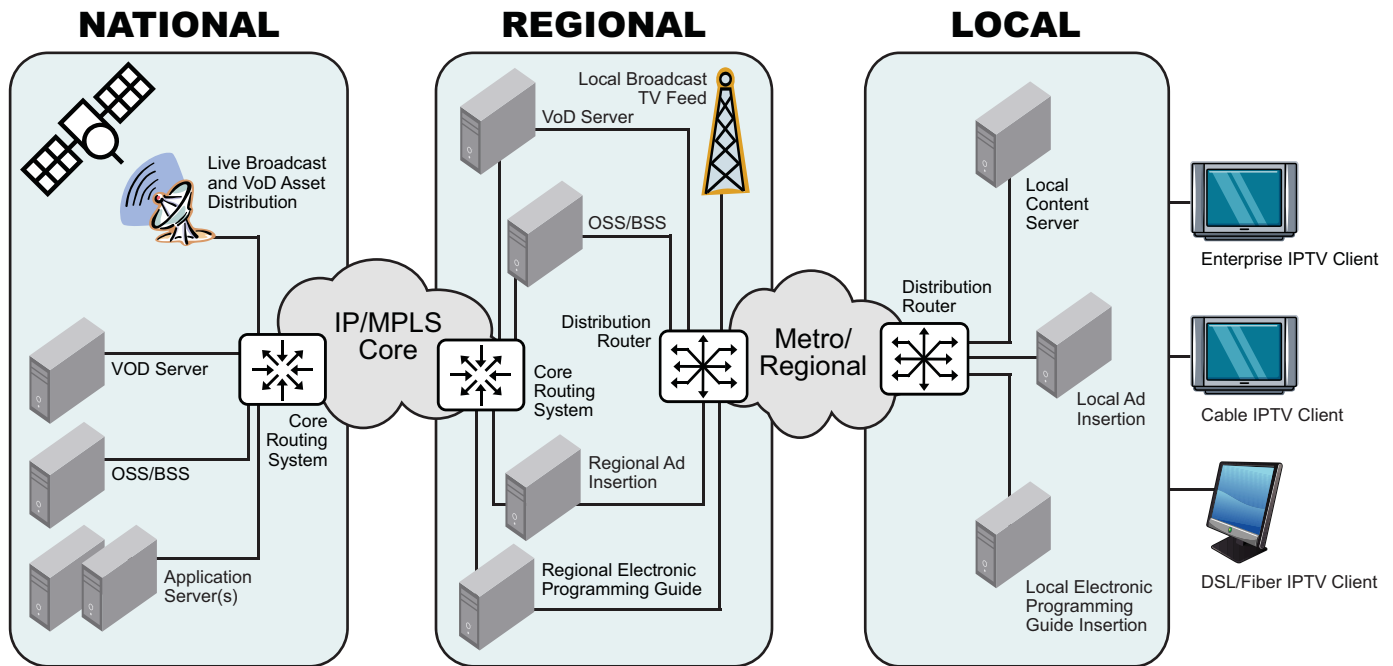


Figure 1. A leading service provider's IPTV architecture.

Business Benefits from Mu

The service provider has achieved measurable business benefits with Mu. Comprehensive security and robustness testing is incorporated into the IPTV deployment lifecycle, from product purchasing to deployment to product updates. The service provider has met its goals for IPTV service uptime and has avoided unplanned service disruptions or quality issues that can negatively impact revenue, customer retention rate, customer satisfaction and the public perception of its IPTV service.

Key results include:

- Rolled out IPTV pilot that met its customers' expectations as well as service level agreements for availability and quality.
- Reduced cost due to a proactive approach to problem resolution.

Reducing Total Cost of Ownership

Lower total costs contribute to a faster ROI, especially considering the significant investment required for a digital TV infrastructure. Firstly, the provider has saved on equipment outlay, lowering its capital expenditures (CapEx). Mu provides an integrated analysis approach, so the service provider does not need to buy multiple point solutions that provide a fraction of the analysis capabilities of Mu.

It has also reduced operational expenses (OpEx) for the IPTV infrastructure, due to cost savings in problem resolution and avoidable support costs. With Mu's full range of remediation tools, interactive charts and detailed reports, resolving issues with vendors has become easier and less time-consuming. The engineering team uses Mu to find bugs before service roll-out and upgrade, so the frequency and severity of downtime has been reduced. Customer service and network support staff spends less time resolving downtime-related customer issues.

Layer	Network Elements	Mu Tested	Benefits from Using Mu
National	Core routers	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Harden IPTV infrastructure • Reduce TCO by addressing product vulnerabilities early • Deliver high quality video
	Video Servers	<input checked="" type="checkbox"/>	
	CMTSs	<input checked="" type="checkbox"/>	
	Subscriber Management System	<input checked="" type="checkbox"/>	
Regional	Core routers	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Minimize quality issues, including packet loss and jitter • Characterize system responsiveness to identify problem spots
	Video Servers	<input checked="" type="checkbox"/>	
	CMTS	<input checked="" type="checkbox"/>	
	Subscriber Management System	<input checked="" type="checkbox"/>	
Local	Edge Routers	<input checked="" type="checkbox"/>	
	L2 Switches	<input checked="" type="checkbox"/>	
	Home Gateways	<input checked="" type="checkbox"/>	
	Set-top Boxes	<input checked="" type="checkbox"/>	
	Multimedia	<input checked="" type="checkbox"/>	
	Terminal Adapters	<input checked="" type="checkbox"/>	
	DSLAMs	<input checked="" type="checkbox"/>	

Table 1. Mu's Solution Provides Comprehensive Service Assurance for IPTV Network Elements and Applications.

The service provider delivers IPTV over the same infrastructure as VoIP and other IP services without impacting those revenue-generating services. It has been able to achieve its SLAs, which means it has avoided penalties. Mu's Response Time Charts provides detailed,

actionable information about system response time and availability statistics, making it easy for the service provider to audit its SLA conformance and avoid SLA-related penalties.

The service provider has improved its software patch process as well as its ongoing security operations. Mu's regression testing feature enables its testing staff to accurately verify bug fixes and software upgrades from vendors. Mu's run-to-completion analysis capability does not require human intervention once started, and automatically pinpoints flaws. Mu's analysis templates help disseminate scarce security knowledge, and establish security analysis best practices across the entire organization. The provider finds it easier to train new analysts and provide professional development in security analysis for existing staff.

Technical Details

Thorough Attack Surface Coverage

Mu-4000 analyzer provides comprehensive coverage of protocols used in IPTV. The engineering team subjects IPTV elements and protocols to rigorous attack mutations to discover service availability weaknesses that result from protocol vulnerabilities. The team uses Mu to test IPTV gear, including multimedia terminal adapters, CMTS, set-top boxes, home gateways, subscriber management systems, edge and core routers, L2 switches, intelligent DSLAMs and video services. The Mu can test across a broad array of IPTV protocols, including IGMP, RTSP, SIP, H.248, MGCP, PIM, SNMP, SSH, HTTP and IPv6.

The engineering team uses Mu to detect zero-day and published vulnerabilities in IPTV devices prior to purchase and deployment. Mu's Dynamic Stateful Fuzzing technique subjects the target system to many combinations and permutations of protocol abuse attacks. Fuzzing uncovers problems that are overlooked by conventional testing methods, including buffer overflows, memory leaks, CPU utilization and latency issues, which are critical for video, voice and multimedia applications.

Comprehensive Support for Analyzing IPTV Deployments

Pinpointing vulnerabilities prior to product purchase or deployment clearly improves the network's security posture. With Mu, the service provider can also establish a baseline for the IPTV product security and robustness, which is essential, given the rapid evolution of IPTV protocols and products occurring today.

The engineering team uses Mu as part of its remediation processes. It uses Mu to verify new patches and releases as part of its change management process.

Automation Improves Efficiency

Assessing robustness and security is an inherent part of this service provider's operational best practices and given the massive complexity of IPTV, test automation is a foregone conclusion. The time savings enabled the service provider to roll out IPTV services on budget and on schedule. With automation, they can cover more mutations than would be humanly possible with scripting or manual efforts. They use Mu-4000 appliance to automate other toolsets, including the open-source vulnerability analysis tool Nessus. Another time-saver is the ability to automatically re-run any test with one-touch regression testing, which allows them to validate that a vendor's patch truly fixes the issue.

Ease of Use

The security team also appreciates Mu's GUI for ease of use. As a Web-based appliance, Mu-4000 is easy to install and is intuitive to use. Wizards and templates guide the engineers through the analysis process. Creating and using a template is a step-by-step process that allows the engineers to define attack types, monitor events and take action in response to events. Test-center staff simply selects any of Mu's protocols and then configures the comprehensive variety of custom attack parameters in each template.

The XML-based templates are also portable using Mu-4000 for any aspect of the analysis. Templates further a "Best Practice" approach that is easily shared organization-wide and with the engineers that have complementary skill sets. Monitors allow engineers to capture additional information on the target, so they can capture exactly what was happening at any moment to trigger automatic fault isolation.

Ongoing Analysis

By verifying that vulnerable IPTV products are not deployed into production, this Tier-1 service provider avoids most significant problems down the road, including service degradations and downtime. Mu-4000 is used across the entire deployment lifecycle from the initial product purchase to subsequent upgrades.



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317

CASE STUDY: Bolstering the Reliability, Availability and Security of IP Multimedia Subsystem (IMS) Rollouts by Security Assurance

The Service Availability Challenge

IMS is being quickly elevated in carrier spending priorities for its promised ability to transform the telecom industry. Telcos, mobile operators and other service providers want to deliver multimedia services across next-generation packet-switched networks and traditional circuit-switched networks, including mobile networks (e.g., GSM 3G, LTE, WiMAX, etc.). Service providers expect and require that their significant investments in IMS will quickly reap new business opportunities and lower operational costs without placing existing services at risk. But before new multimedia services become a strong revenue contributor, service providers and network product providers alike must have strong confidence in the reliability, availability and security of the underlying IMS infrastructure.

One major international service provider is well on its way to reaping the rewards of IMS. This Tier 1 service provider is piloting IMS-based services, including VoIP, presence and other advanced applications. Based on the success of its pilot, an aggressive schedule is underway for interactive push-to-talk, multimedia conferencing and other multimedia applications.

High Cost of Downtime

Customers expect dial-tone when they pick up their phone (be it a handset, a smartphone or a softphone), and they will not dismiss reliability for the pleasure of cool multimedia applications. If service providers want to maintain loyal subscribers and protect their brand, they need to meet the wireline carrier industry's gold standard of 99.999% uptime, regardless if services are traditional or cutting edge.

Absolute failures continue to be of major concern, but service providers must also contend with partial failures or service degradations, where a service performs more slowly than usual, even to the point of end user frustration. Downtime in IMS-based services can result in significant lost revenue for the providers because of:

- customer churn,
- increase in avoidable support costs,
- decreased average revenue per user (ARPU).

Loss of Service Revenue

This service provider estimates that, in a small metropolitan area with 100,000 subscribers, downtime in its residential service areas costs more than \$8,300 per hour and that downtime in business service areas costs more than \$11,500 per hour. Across all its service areas, the cost of downtime quickly adds up to **tens of millions of dollars per year**.



EXECUTIVE SUMMARY

CHALLENGE

- Capture new revenue opportunities and reduce operational costs by transitioning to next-generation network architecture and IMS;
- Offer VoIP, presence-based applications, multimedia conferencing and other advanced services that are reliable, available and secure;
- Identify and eliminate sources of potential service degradations before they impact the customer experience and service-level agreements;
- Select high-quality IMS products free from service-affecting vulnerabilities that may result in downtime.

SOLUTION

Mu-4000 Analyzer

RESULTS

- Met service availability requirements for VoIP and rich media applications;
- Met aggressive rollout schedule for IMS applications and pilot of next-generation network architecture;
- Verified that IMS products are free from security or reliability weaknesses before products are purchased and deployed into the production network;
- Automated and conducted comprehensive testing of highly complex IMS applications and equipment, and integrated into regression testing across the whole deployment life cycle.

business-critical voice service. If an attacker used SIP to disable a security enforcement device, the service provider's entire perimeter defense system is compromised and the attacker may access the service provider's core network to inflict further disruptive behavior. Loss of these services will negatively impact providers' service availability and revenues.

Improving Service Availability and Security with Mu

The Chief Architect of IMS Services at this service provider is keenly aware that delivering a useful, profitable service to customers also means protecting the IMS against attacks and service abuse. Verifying that IMS products are free from zero-day and known vulnerabilities is a vital step in this protection. The Chief Architect demanded that all gear deployed in the IMS pilot meet the company's same high standards for reliability, availability and security as the traditional circuit-switched network. The solution was the Mu-4000 appliance and its SIP protocol mutation modules for comprehensive service assurance. Figure 2 shows a simplified network diagram of this service provider's IMS architecture. Table 1 summarizes the network elements that the Mu solution analyzes and the benefits for the service providers. Please refer to the "Use Case Details" section for more information.

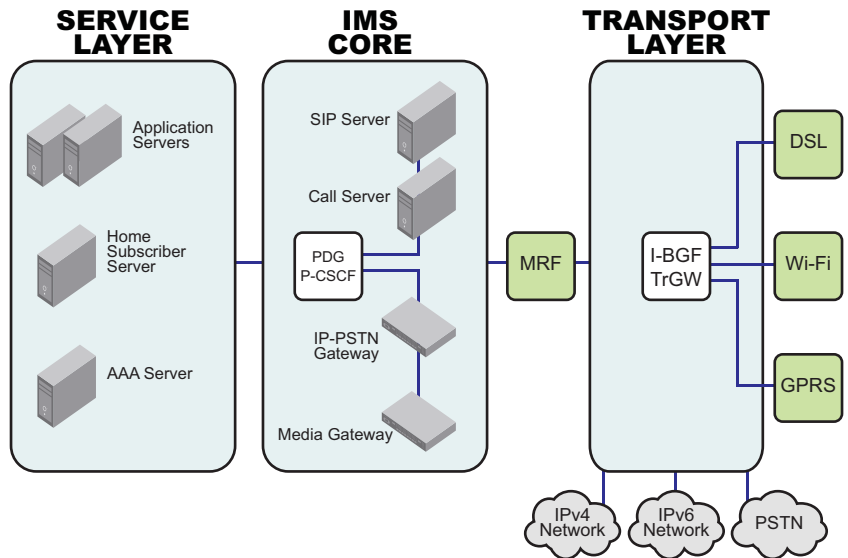


Figure 3. A leading service provider's IMS architecture.

Business Benefits from Using Mu

After using Mu's solution for nine months, the service provider achieved significant business benefits. With comprehensive service assurance incorporated into the entire life cycle of its IMS deployment, the provider met its goals for service uptime and avoided service disruptions or quality issues that would otherwise impact revenue, customer retention rate and overall customer satisfaction.

Key results include:

- Minimized system downtime and associated customer churn.
- Rolled out IMS applications met or exceeded customers' expectations as well as internal metrics for service availability and quality.
- Reduced cost in several operations areas due to taking a proactive approach to problem resolution before IMS network infrastructure was production deployed.

Reducing Total Cost of Ownership

Gaining cost efficiencies are especially important, given the investment required to build-out an IMS infrastructure.

CapEx | The provider saved on capital equipment expenditures with Mu's solution. Mu helps this service provider ensure the IMS products and applications it purchases are resilient, which prevents wasting valuable CapEx on low-quality products, also avoiding OpEx penalties due to higher-than-planned field fire drills of lower-quality equipment in production deployment. Mu provides an automated analysis approach, so the service provider does not need to buy multiple point solutions providing only one component of the necessary service assurance analysis capabilities of Mu.

Layer	Network Elements	Mu Tested	Benefits from Using Mu
Service/ Applications Layer	Application Server	☑	<ul style="list-style-type: none"> • Harden IMS Service infrastructure • Protect against vulnerabilities that may result in voice spam, denial-of-service attacks and malware.
	Home Subscriber Server	☑	
	Authentication Authorization Accounting (AAA) Server	☑	
	Media Resource Function (MRF) Server	☑	
	Security Gateway	☑	
IMS Core (Control) Layer	Call Session Control Function (CSCF)	☑	<ul style="list-style-type: none"> • Reduce TCO by addressing product vulnerabilities early. • Characterize system responsiveness to identify problem spots.
	Packet Data Gateway (PDG)	☑	
	SIP Server	☑	
	Call Server	☑	
	Media Gateway	☑	
	IP-PSTN Gateway	☑	
Transport Layer	Interconnection Border Gateway Function (I-BGF)	☑	
	Translation Gateway (trGW)	☑	
	Router	☑	

Table 1. Mu's Solution Provides Comprehensive Service Assurance for IMS Network Elements and Applications.

Loss from Customer Churn

The service provider further estimates that, in the average small metro area, dissatisfaction with the quality of an existing service increases the customer churn rate by up to 5 percent. Service reliability is even more important when piloting new services, since users are forming their first impressions and the success of the broader business is at stake. So for the IMS pilot, the service provider estimates that customer dissatisfaction will increase the churn rate up to 8 percent.

The service provider conservatively estimates that the cost of churn per subscriber ranges from \$400 to \$600, based on time-based replacement costs. Figure 1 shows just how expensive it is for the service provider when customers become unhappy to the point that they leave for an alternative carrier. The average cost of churn for this small metro area would range from \$1.6M to \$4.8M per year. Again, across all the regions serviced by this provider the cost of customer churn quickly grows to **hundreds of millions of dollars per year**.

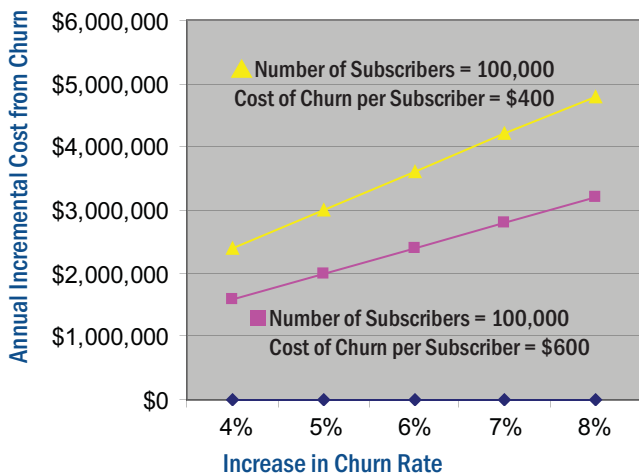


Figure 1: Cost of customer churn as a result of IMS quality issues in a small metro area of 100,000 subscribers.

Difficulties in Testing IMS Networks

Due to these high costs, service providers are motivated to reduce network downtime and maintain high IMS service quality. However, assuring the reliability, availability and security of emerging IMS services is an unprecedented challenge. Balancing the economic and competitive pressure to deploy new services at traditionally high subscriber expectations over a rapidly changing infrastructure is like nothing that has been attempted by the carriers. Addressing the challenge requires expertise and solutions previously unavailable in the industry. These solutions must methodically measure and assure the service availability of an IMS network and its associated applications, from transport to core to application services. This service provider understands firsthand that the inherent complexity and immaturity of IMS create ample opportunities for interoperability and robustness issues.

New and Complex

IMS is comprised of dozens of new protocols specified by many standards bodies, including the 3rd Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), International Telecommunication Union (ITU), the IMS Forum, and CableLabs. Any new protocol or protocol extension may have many interpretations and carries the risk of being fragile (and causing operator network downtime) until hardened in the real world.

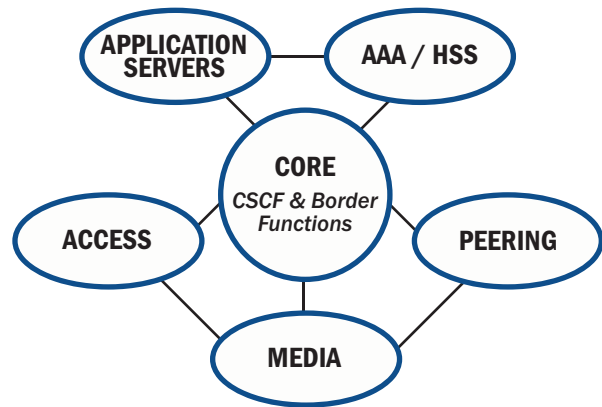


Figure 2: Generic IMS architecture. The number of protocols required by IMS networks is exponentially multiplied by many different types of equipments and applications. The variety of deployment scenarios further adds to the complexity.

In addition, IMS leverages many IP-based protocols, each of which has its own dependencies and vulnerabilities. For delivering voice [over IP] service, IMS uses the Session Initiation Protocol (SIP) to control communications. SIP is known to have a large number of acceptable implementations, which creates unforeseen security weaknesses and makes it challenging for network equipment manufacturers to build interoperable products. SIP itself leverages many of the mechanisms developed for HTTP and SMTP/MIME, thus inheriting those protocols' weaknesses and vulnerabilities as well.

Fragile and Vulnerable

VoIP communications from subscribers' PCs, smartphones and other SIP endpoints on a next-generation network are far more exposed than traditional analog communications. Attacks may originate from the Internet, wireless LANs or GPRS networks.

Attackers potentially compromise applications using IMS and SIP, such as presence-based applications, to bypass traditional perimeter network defenses and spread spam/spit (spam over Internet telephony), denial-of-service (DoS) attacks, malware or worse. Malicious traffic, including DoS flooding attacks can severely impact voice quality, as VoIP is far more sensitive to network latency and jitter than "best-effort" data-oriented applications. If any IMS vulnerabilities are exploited, attackers could knock out a media gateway, voicemail, or other

OpEx | The provider also saved on operational expenses after leveraging the automation and ease of use of Mu's solution. Resolving vulnerability and bug fix issues with vendors now involves less finger-pointing and is quicker, because of Mu's full range of remediation tools, interactive charts and detailed reports, highlighting the issues in detail. The testing staff accurately verifies bug fixes from vendors with Mu's regression testing feature. The service provider also reduces costly SLA penalties using Mu's Response time Charts for highly actionable information about system response time and availability statistics available.

Use Case Details

Testing IMS Transport, Core and Services Layers

This service provider uses the Mu-4000 analyzer to test the reliability, availability and security of gear used in the IMS transport, core and services layers. Comprehensive test coverage across all involved IMS network elements is essential because any single protocol vulnerability can expose the entire network to attack.

With Mu, the service provider's engineering team detects zero-day, DoS and published vulnerabilities in VoIP and IMS products. Mu is an integral part of the service provider's life cycle for IMS product purchase, development, roll-out and change management. When vulnerabilities or product weaknesses are identified through use of the Mu system, the onboard Mu remediation suite is essential for efficient problem resolution. Automated testing with Mu saves the engineering team considerable time, which enabled the service provider to roll out IMS applications to customers on schedule.

The Mu-4000's Dynamic Stateful Fuzzing engine subjects the target IMS system to many combinations and permutations of protocol attacks in a controlled environment. Fuzzing, combined with an advanced monitoring and fault isolation capability, uncovers problems that are often overlooked by conventional testing methods but are particularly important for voice and real-time multimedia applications. These issues include:

- buffer overflows,
- memory leaks,
- CPU utilization spike,
- performance degradation, and
- other latency issues.

IMS Core Layer

The engineering team uses the Mu-4000 to test the Proxy Call Session Control Function (P-CSCF), which acts as a centralized SIP routing engine, policy manager and policy enforcement point for the delivery of real-time IMS applications. Protecting the [P-]CSCF from accidental misuse or intentional attacks and is a priority, because attackers can use subscriber devices to attack the IMS edge with DoS attacks, carefully crafted exploit code or malicious packets.

The engineering team also uses the Mu-4000 to test the IP-PSTN gateways, media gateways and perimeter security devices. The Interrogating Call Session Control Functions (I-CSCF's) that serve as the SIP peering point between service providers are also a point of potential exposure. One service provider may inadvertently pass malicious traffic across the SIP peering links or even everyday network packet corruption could impact service availability. The engineering team uses the Mu-4000 to assure that the I-CSCF's are robust.

Application Layer

The team also uses the Mu-4000 to test availability and robustness of various IMS services, including application services for VoIP, push-to-talk and multimedia conferencing. Engineers use the Mu-4000 to test interactions between the Serving Call Session Control Function (S-CSCF) in the control layer and the Application Server functions. Developers' ability to test XML and HTTP/HTTPS protocols is also essential for applications that use web services to take advantage of IMS network functionality, such as call control, conferencing and user interaction.

Transport Layer

The provider's test suites using the Mu-4000 typically include SIP with IMS extensions, MGCP, possibly with the NCS profile, H.248 with IA profile, HTTP, XML and RTP. The engineering team uses the Mu-4000 to test the core infrastructure, including routing protocols, LDP, MPLS, and other lower layer protocols. The engineering team also uses the Mu-4000 to test SIP implementations used in the various endpoint devices. Furthermore, the Mu solution is used to test the H.248 protocol implementations used in the Media Gateway Controller to support voice and fax calls between the PSTN and IP networks, as well as RTP protocols that carry the data encoded with the codecs that digitally represent audio and video traffic.



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317