# MIMIC®

*Simulator*

# Testing the Limits

***Enterprise Network Management, Testing and Evaluation***

**Gambit Communications®**
76 Northeastern Blvd, Suite 29A
Nashua, NH 03062
www.gambitcomm.com
(603) 889-5100

**Gambit Communications, Inc.**

Founded in 1995, Gambit Communications is a leader in network simulation tools that enhance the productivity of management software developers and enterprise users while lowering their costs. MIMIC Simulator is a modular family of simulators used by leading networking vendors for use in applications from development and testing to operator training and disaster simulations. Gambit Communications' portfolio of many customers includes: IBM, Computer Associates, Hewlett Packard, MCI, Cisco, Nortel, Alcatel-Lucent, Marconi, Intel, Motorola, BMC, Microsoft, Dell, and Ericsson. For more information on Gambit and MIMIC, please visit www.gambitcommunications.com.

Gambit
Communications®

76 Northeastern Blvd., Suite #29A
Nashua, NH 03062
(603) 889 5100
Fax 603-889-5005
www.gambitcomm.com

# Table of Contents

## SUMMARY

*Effective testing and evaluation can significantly improve enterprise network management, which in turn can positively impact a company's day-to-day operations and financial performance. After a network failure, it is too late to suggest that an evaluation policy should have been implemented — the damage has been done. In addition, management wants to ensure that their networks will survive a disaster scenario (such as power outages, earthquakes and fires). Ensuring the viability of new network management system (NMS) applications, new network devices and proposed management policies, however, can be a very cumbersome task. Many companies still rely on physical labs, which are smaller scale copies of their production networks. The physical lab has both logistical and financial limitations. Realizing these issues, Gambit Communications® introduced a solution with MIMIC® Simulator. The creation of a virtual lab with MIMIC and how this can address the needs of various companies, from evaluation, testing and disaster simulations to software development, partner support and certification, is the subject of this paper.*

# INTRODUCTION

## What is SNMP?

A significant issue within network management had been the need for a common protocol for NMS applications to communicate with manageable network devices. This need prompted a group of computer scientists, including Jeff Case, Marshall Rose and Ken Key, to address this issue. In 1988, they created the simple network management protocol (SNMP).

SNMP represents the *de facto* standard protocol used for network management and the monitoring of network devices and their function. Every SNMP-managed network consists of two key components: managed entities and NMS applications.

Every managed device (routers, servers, switches, bridges, hubs, computer hosts, cable modems, printers, etc.) on the network has an agent, which is a small software module that monitors and tracks local management information. The agent stores this information in a management information base (MIB) and makes it available to the NMS by communicating through the SNMP protocol. The NMS uses this information to monitor and control the networked devices. In this way, SNMP provides the means necessary for a network management system to communicate with all the networked devices within an enterprise-wide network or for an element management system to communicate with specific, proprietary hardware.

Since its inception, SNMP has evolved and increased in functionality. Three versions of SNMP are currently prevalent: SNMPv1, SNMPv2 and SNMPv3. All these versions conform to the specifications of the structure of management information (SMI). SNMPv1 represents the initial implementation of the protocol. It operates over protocols such as User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP/IP), OSI Connectionless Network Service (CLNS), AppleTalk® Datagram Delivery Protocol (DDP) and Novell Internet Packet Exchange (IPX). SNMPv1 has also become the network management protocol for the Internet community. SNMPv2, originally published and proposed as a set of Internet standards in 1993, represents the second generation of the SNMP protocol. It implemented various improvements, including additional protocol operations. The third generation protocol formalizes many aspects of the protocol, including security, acknowledged traps, etc.

## Enterprise Network Management

In a world of increased Internet connectivity and with the rise of e-commerce, enterprise management has emerged as an increasingly important discipline. The term "network management", however, creates different images in peoples' minds. For some this is a network administrator at a small company managing five computers on an Ethernet. For others it is a series of administrators in a Fortune 500 company managing WANs, LANs and all the associated devices. Yet for others it can be a management service provider (MSP) managing various clients' networks from a central location. Despite these varying scenarios, they all share some basic characteristics — they all use at least one NMS application and a variety of network resources to be managed. In addition, the underlying principles are the same for everyone: network integrity remains essential, and network performance can greatly impact the company's revenue stream.

The traditional model of network management is a company with an internal IT organization that purchases, installs and maintains network devices in addition to administering NMS applications and services. Over time, however, the models of how network administrators accomplish this task have also increased. These include **element management**, **discovery management**, **event-correlation management, service-level management** and **root-cause analysis management**.

**Element management** is associated with proprietary hardware devices. Some hardware vendors create management applications designed to interact specifically with their own devices. The element management paradigm, therefore, consists of an element manager or a series of element managers communicating with their associated devices. In turn, these element managers may be integrated into a management framework in order to interact seamlessly with the entire network environment.

The **discovery management** tool detects elements on a network. This provides limited information, such as IP addresses, the device name and the device's configuration. Using this method, an administrator can create and view a network topology. However, the discovery process does not provide any information about how or if the device is functioning.

**Event-correlation management** helps control the flow of information in the case of specific events. For example, if on a large network a router were to fail, the router itself would send an error message; however, many of the devices relying on this router would also broadcast error messages. No network administrator wants to receive hundreds of error messages, because of a single device failure. Event-correlation tools, therefore, can suppress the majority of the error messages associated with this failure and send only the necessary information to the NMS application.

**Service-level management** entails setting specific network management service goals and managing the networks to meet those goals. This allows for more effective network management, since selected metrics can be compared against the goals. If the metrics vary significantly from the goals, then network administrators can administer new policies to address these issues. This in turn allows for more cost effective management by being better able to use network resources.

By quickly identifying the root-cause of a problem within a network, **root-cause analysis management** helps to minimize the resources necessary to address these problems in a timely manner. With a root-cause management system in place, a network administrator can take proactive steps to look for potential root-causes. The administrator can then predict the impact of potential problems on the network and plan for solutions if such a problem arises.

### *The Challenges in Enterprise Network Management*

The introduction of SNMP has significantly improved network management, but has not in itself ensured network integrity. Having recognized this, numerous software and hardware developers exist that constantly strive to provide better network management solutions. As they create these new programs and devices, it is important to ensure that they will work properly within a wide variety of network environments. How can this be done? Particularly, since without a guarantee of interoperability, very few customers will be interested in the new technology.

This is compounded by other challenges to enterprise network management, especially within an environment of increased corporate dependence (even in small companies) on networks. Unlike many other industries where economies of scale provide more and more advantages, in the world of network management as the size of the network increases so do the associated complexities.

One of the most obvious issues facing the network management sector is the proliferation of "intelligent" network devices. On an SNMP-managed network, each manageable device has an associated SNMP agent and associated MIBs either embedded in it or hosted on another device, such as a workstation. Therefore, a network administrator needs to worry about supporting an ever-increasing number of devices. In addition, the device vendors frequently release agent and MIB updates, which can cause network maintenance headaches.

The increasing number of manageable network devices in turn leads also to problems as basic as setting up and maintaining the infrastructure of the network. Due to the fact that so many hardware vendors exist, there also exists a combinatorial explosion of scenarios. This can cause many problems for network management, such as a recent widely publicized report where an improperly configured device crashed an entire network. In addition, with the rate of technological obsolescence, it is necessary to upgrade network devices constantly.

Managing this multitude of heterogeneous devices can also cause financial strains on an organization. Not only is it extremely expensive to try to keep up with the latest technology, an extensive network also represents the associated support costs necessary to keep it functioning properly. In addition, planning for future growth is difficult, because with tightening profit margins, it becomes more and more difficult to justify the purchase of additional equipment and to hire additional staff to administer the network.

All of these factors can lead to the inefficient use of network resources. In addition, before implementing a new NMS application, adding more devices to the network or instituting new policies, companies need to be assured that this will not adversely affect the network. NMS application developers and hardware vendors have encountered a similar problem trying to address this issue: how can they ensure that their products will adequately communicate with, interact with and manage all these devices.

## TESTING AND EVALUATION OF MANAGEMENT APPLICATIONS

Until recently the choices for testing and evaluating real-world network situations have been very limited. There have been basically only two options: perform tests on the production network or create a separate physical test lab. The first option creates very serious concerns, since a network failure can result in very negative financial consequences. No company wants to risk its production network's integrity for testing purposes. Secondly, the tests would need to be performed during off-hours in order not to disrupt the company's day-to-day operations; however, in today's internet-driven economy, many companies' networks are in operation 24/7. Given these factors alone, testing on the live production network has not proven to be a viable option. Therefore, companies have had to rely on isolated lab environments, which were normally small-scale facsimiles of their enterprise-wide networks.

### *Physical Labs*

Network laboratories have played a vital role not only in testing, but also in the development, training and certification of site-specific management policies for NMS applications. These environments provide a test-bed outside of the live, production network for the development and testing of new applications for the support of specific devices, networks, topologies, scalability, the handling of crisis scenarios and training customers. However, there are certain difficulties associated with the physical lab that create significant barriers to effective and timely development cycles, such as the physical lab's complexity, capacity limits and availability.

System administrators and software engineers have the difficult task of acquiring devices in order to provide an appropriate lab environment that reflects the enterprise network environment. The time to research, budget, purchase, install and inventory hardware consumes human and capital resources — resources that could be used more effectively.

In most cases several groups must share the same lab for varying purposes, which adds to the complexities of a physical lab. In an enterprise, the sales team may need to create product demos. On the other hand, the network administrators may want to evaluate new NMS applications or management policies before implementing on the production network. On the development side, QA personnel testing new releases of applications may require a sizeable network, for example, to test the scalability of the application. A developer may require reproducing fault conditions to ensure the proper functionality of new features. In this environment, each team spends significant time setting up, configuring and maintaining the lab equipment, taking time away from their respective objectives. This time and resource sharing between multiple groups can also impact development schedules.

In addition, for software developers and device vendors, software engineers need the appropriate devices in order to perform their development work. Device availability becomes rare, especially if the device is still under development or has to be acquired from outside sources. This is magnified when the application is required to support third-party vendor hardware.

In general, even though the physical lab has provided a better option for testing than possibly compromising the production network, it still has limitations associated with it. Some of these limitations include the financial impact of constantly purchasing new devices as they reach the market; the administrative headaches of maintaining the lab and the equipment; the varying requirements of the labs users; and gaining access to the lab due to scheduling issues.

### *Virtual Lab with MIMIC*

In September 1997, Gambit Communications introduced an alternative solution for this problem with the MIMIC™ Simulator. Today many NMS vendors have implemented the use of MIMIC. It extends the lab environment by simulating thousands of SNMP (v1, v2 and v3) manageable devices. Companies have discovered that with MIMIC, they can provide each developer, tester, trainer and salesperson a private, virtual lab. This alleviates the overhead and administrative headaches of physical equipment, increases efficiency and significantly expedites the software development cycle.

**In addition, MIMIC overcomes the financial and resource constraints by allowing users to set up virtual labs that are much more extensive than could be available with physical labs. MIMIC is targeted at testing and demonstrating NMS applications for scalability, robustness, performance and effective policy implementations.**

### *What Is a Simulation?*

A simulation is the act of exporting MIB object instances and values, just as a real-world manageable device does, but without the actual physical device. The network management application interacts with the simulations within MIMIC just as it would with real-world devices. The most common is a “realistic” simulation, i.e., it attempts to duplicate the behavior of a real-world device. Realistic simulations are good for demonstrating the capabilities of a network management application in a pre-sales situation, or as part of training exercises.

For a particular device, any number of simulations can be run, just as in the real world there are a number of scenarios in which a device can be involved. For example, the user can create a router simulation of a lightly loaded device or an overburdened device, or any range of scenarios in between. Or, the user can simulate an RMON probe on a healthy network segment, or a probe that is monitoring a segment with either a high traffic load or failing devices. From a network management perspective, the difference is seen merely in the instances and values of returned MIB objects.

Simulations with randomness have their limitations in the case of product development and testing, because the values of MIB objects are unpredictable. For this use, MIMIC allows the creation of “constant” simulations. This type of simulation makes counter objects return a value with a constant rate.

### *The Value of MIMIC Simulator*

Using MIMIC to create a virtual lab represents a significant value proposition for an organization. Some examples of this are as follows:

- Reduces hardware costs by a factor of 10 to 1,000;
- Provides total **cost savings of 92%** over a physical lab, based on 100 devices;
- Saves the time and costs of engineering labor;
- Creates large-scale, multi-vendor labs that would otherwise not be possible;
- Produces realistic, unforeseen and disaster scenarios that could take months to produce in a physical lab;
- Reproduces those scenarios when need for regression testing, demos and training;
- Diminishes sales and marketing expenses to produce powerful product demos;

- Determines an NMS application’s optimum performance before deploying it;
- Trains each new engineer on the appropriate NMS applications in their own private, virtual lab

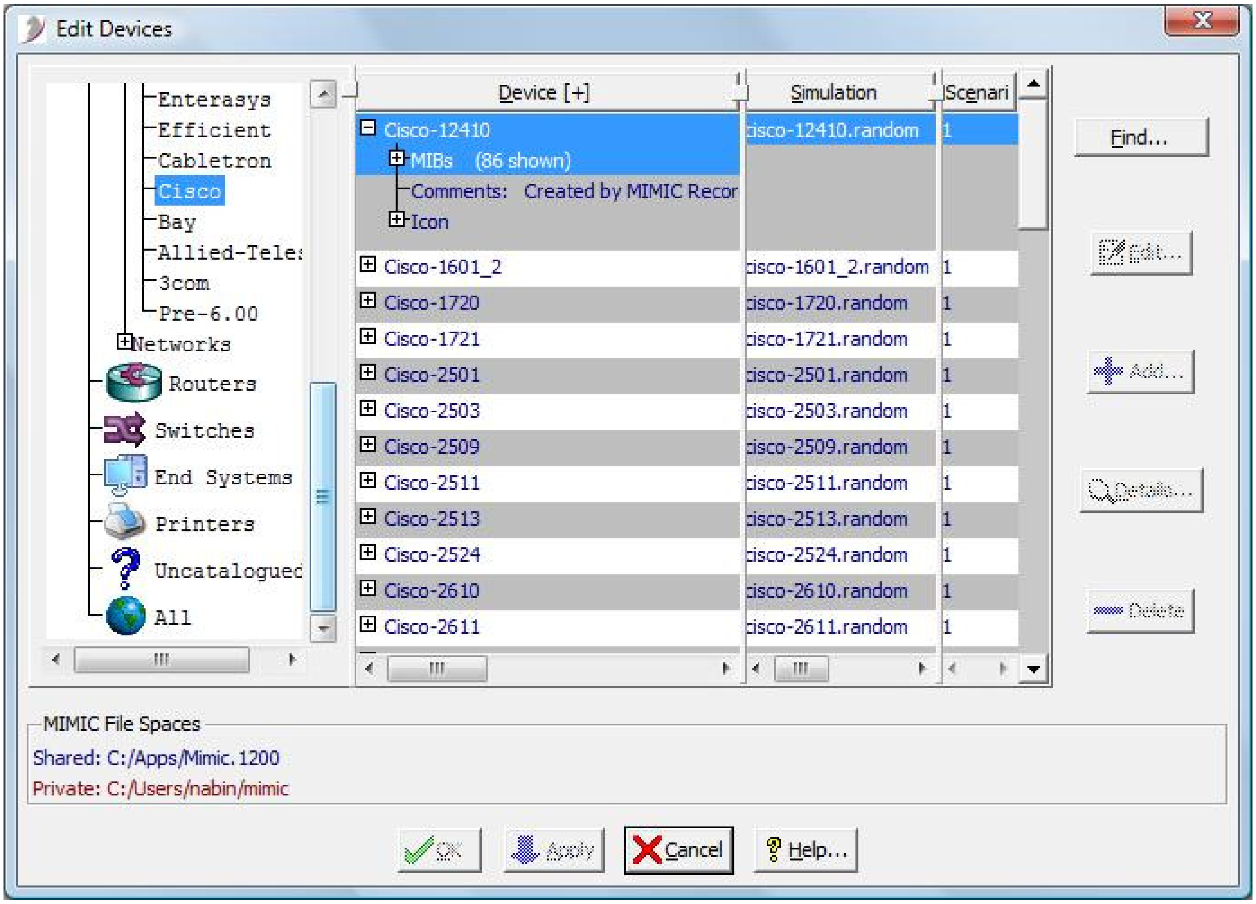
## MIMIC'S CAPABILITIES

**Real-time monitoring/management:** Users have the ability to instantiate quickly new devices or entire network segments, individually or in groups, and schedule network "scenarios" that change SNMP variables, start or shut down devices, or generate traps. Multiple network management tools can query the same MIMIC simulated devices, each with its own unique simulated network view.

**Network configuration "capture and playback":** Actual network configurations are easily produced. MIMIC Recorder can take a snapshot of the device management information base (MIB) and then "replay" it instantly in the lab. It can also make controlled adjustments to SNMP variables to recreate problems or to test configuration variations. With MIMIC, the production network is recreated in the lab!

**Custom simulation:** With the intuitive graphical user interface (GUI) or flexible scripting language, MIMIC offers complete control of the virtual network environment. The ability exists to change variable values, such as status, arrival rate and utilization rate for a single device or an entire group. By extending the MIB structure itself, users can create prototypes of brand-new "devices."

**Extensibility:** An extensive MIB library provides out-of-the-box support for leading data network equipment vendors. In addition, MIMIC Compiler easily imports new and custom MIBs to provide complete simulation of any SNMP-compatible device management agent.



| Device [+] | Simulation | Scenari |
|---|---|---|
| ⊟ Cisco-12410 | cisco-12410.random | 1 |
| ⊞ MIBs (86 shown) | | |
| Comments: Created by MIMIC Recor | | |
| ⊞ Icon | | |
| ⊞ Cisco-1601_2 | cisco-1601_2.random | 1 |
| ⊞ Cisco-1720 | cisco-1720.random | 1 |
| ⊞ Cisco-1721 | cisco-1721.random | 1 |
| ⊞ Cisco-2501 | cisco-2501.random | 1 |
| ⊞ Cisco-2503 | cisco-2503.random | 1 |
| ⊞ Cisco-2509 | cisco-2509.random | 1 |
| ⊞ Cisco-2511 | cisco-2511.random | 1 |
| ⊞ Cisco-2513 | cisco-2513.random | 1 |
| ⊞ Cisco-2524 | cisco-2524.random | 1 |
| ⊞ Cisco-2610 | cisco-2610.random | 1 |
| ⊞ Cisco-2611 | cisco-2611.random | 1 |

MIMIC File Spaces
Shared: C:/Apps/Mimic.1200
Private: C:/Users/nabin/mimic

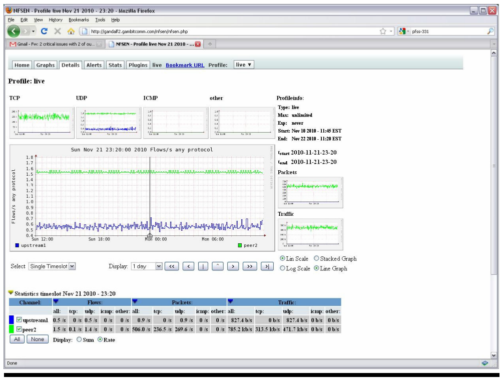
**Scalability:** MIMIC supports thousands of agents on a single server, thus enabling simulation for large enterprise networks. Multiple MIMIC servers can supply unlimited scalability.

**Ease of use:** MIMC provides both a GUI and scripting. Several application wizards in the GUI facilitate initial setup of the simulation, while scripting automates regression testing and demos.

## ADDITIONAL MIMIC CAPABILITIES

### *MIMIC NetFlow/ sFlow/ IPFIX Simulator*

The MIMIC Flow Simulator generates a variety of flows and enables you to fully test your applications. Since you have a complete control over generated flowsets you can easily verify that your graphing application is correctly displaying the values and your collector correctly collects precisely generated flowsets.


NFSEN - Profile live Nov 21 2010 - 23:20 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://gandalf2.gambitcomm.com/nfsen/nfsen.php
pfss-331
Gmail - Fw: 2 critical issues with 2 of ou...
NFSEN - Profile live Nov 21 2010 - ...
Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile: live
TCP
UDP
ICMP
other
Sun Nov 21 23:20:00 2010 Flows/s any protocol
Flows/s any protocol
1.8
1.7
1.6
1.5
1.4
1.3
1.2
1.1
1.0
0.9
0.8
0.7
0.6
0.5
0.4
Sun 12:00
Sun 18:00
Mon 00:00
Mon 06:00
upstream1
peer2
Packets
Traffic
Done

Profile: live

Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Nov 10 2010 - 11:45 EST
End: Nov 22 2010 - 11:20 EST

tstart 2010-11-21-23-20
tend 2010-11-21-23-20

○ Lin Scale ○ Stacked Graph
○ Log Scale ● Line Graph

Select: Single Timeslot
Display: 1 day

Statistics timeslot Nov 21 2010 - 23:20

| Channel: | Flows: | | | | | Packets: | | | | | Traffic: | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| ☑ upstream1 | 0.5 /s | 0 /s | 0.5 /s | 0 /s | 0 /s | 0.9 /s | 0 /s | 0.9 /s | 0 /s | 0 /s | 827.4 b/s | 0 b/s | 827.4 b/s | 0 b/s | 0 b/s |
| ☑ peer2 | 1.5 /s | 0.1 /s | 1.4 /s | 0 /s | 0 /s | 506.0 /s | 236.5 /s | 269.6 /s | 0 /s | 0 /s | 785.2 kb/s | 313.5 kb/s | 471.7 kb/s | 0 b/s | 0 b/s |

All None Display: ○ Sum ● Rate

**Flow Simulation:**

- **Configuration** - Configure simulated NetFlow devices to create exactly how you want to show your network's functions (how it is used, by whom, and for what purpose).
- **Correlation** - Test the correlation of the traffic arriving from designated ports, source/destination IPs and protocols.
- **Traffic generation** - Create a comprehensive view of your simulated network traffic, with bottlenecks and bandwidth hogs.
- **Customize the simulation** - Start using without any customization or fully customize any/all flow record values.
- **Flow changes** - Prove that value changes are detected according to the specified rules.
- **SNMP to NetFlow** - Change SNMP values of the devices and report those results in the Flow applications.
- **NetFlow to SNMP** - Change Flow values of the devices and report those results in the SNMP based applications.

The MIMIC NetFlow Simulator, the industry's first integrated simulation tool supporting NetFlow, sFlow, IPFIX and SNMP, allows developers to perform real world, integrated device simulations. MIMIC simulates NetFlow-capable networking devices. MIMIC allows suppliers of NetFlow devices and applications to design, develop and test their products in a virtual and scalable network environment, assuring customers that their applications will work properly when deployed across heterogeneous environments.

## MIMIC'S APPLICATIONS

MIMIC provides the ability to reduce total cost while increasing efficiency in several functional areas of a network management product's lifecycle. Some of these areas include R&D, sales and marketing, quality assurance (QA), support, training and evaluation. Following are various examples of MIMIC's applications in these areas:

### *Disaster Simulation*

Disasters that impact networks take many forms – from natural disasters like earthquakes and fires to line cuts. Many companies conduct disaster planning for their networks. The threat of a network outage is real, and networks are vital to the health of companies. Major network outages can adversely impact departments from product development to customer services and cause loss of revenue, delays in getting products to market and decreased customer satisfaction. In addition, if the company is an outsourcer providing network management services, an outage means not meeting a service-level agreement and possibly incurring huge penalties.

However, after disaster planning and creation of a disaster response procedure, how can companies verify that the response procedure will be effective? Using the production network for practicing disaster readiness clearly presents a problem. If the network is used for disaster preparedness practice, the timing of that practice must be carefully chosen. This often requires employees to be available outside the normal hours of operation – a huge imposition for most people. In addition, the time to plan and execute a disaster practice is monumental due to concerns about harm to the network.

The good news on this front is that disaster recovery procedures can now be performed on a simulated network – one that cannot be harmed by the exercise. MIMIC and its SNMP agent recording and simulation capabilities enables this. To set up a disaster preparedness test, companies simply use MIMIC to record their current network and then use that recording in a simulation of the network. The virtual, duplicate network is then available for the practice of disaster recovery scenarios. This not only protects the "real" network safe from this practice, but the participants gain real-world experience in disaster response. The simulation is also available for training and more practice sessions, when personnel turn over. MIMIC provides an effective solution for practicing disaster preparedness!

### *Employee Training*

Providing employee training poses a problem for all companies. Everyone understands the benefits of employee training in allowing employees to perform their jobs with greater success. This, however, represents an expense to the company, as opposed to customer training which generates revenue. There is constant pressure to minimize costs, which often limits the number of seats in training classes available to employees. Even companies that are large enough to have separate employee and customer training facilities find that the employee facilities are treated as second-class, receiving hand-me-down network devices and other materials.

Where the new products are networking devices or network management software, the employee training problem is compounded. Company personnel need to get up to speed quickly in order to perform their jobs with the new product, whether they are in technical support, sales or marketing. How can companies meet the challenge of providing training for company personnel on new products?

For hardware vendors, employees need to be familiar with the new hardware and its management software before it hits the market. They need to know how to install it, use it, troubleshoot it and sell it. However, quantities of the product simply are not available for use in training labs. For network management software vendors, the challenge is providing a multi-vendor, heterogeneous network that is extensive enough to experience fully the software's capabilities. However, providing such a network is cost-prohibitive, not to mention the on-going maintenance and administration costs.

Fortunately, both situations can be resolved through the use of MIMIC's SNMP agent simulation capabilities. MIMIC provides virtual devices that can be used to set up training lab networks. These virtual lab networks can become as extensive and complex as the trainer would like, which allows them to teach fully the capabilities of the element manager or network management application. Network management platforms and today's emerging point solutions have extensive capabilities that scale for use by enterprise customers. Having access to an unlimited number of virtual networking devices allows the trainer to properly represent these capabilities in labs and demonstrations. Plus with MIMIC, students get the opportunity to practice "real world" scenarios – both positive and negative – that would be impossible with a physical network.

MIMIC's ability to provide virtual devices allows students to gain real experience working with large networks and to comprehend fully the value and capabilities of the software. They are able to practice network monitoring and management techniques, troubleshooting skills that they will use with clients, and even experience what it is like to be on the customer side of using the product.

By using MIMIC to provide employee training, companies experience a substantial reduction in expenses associated with their training lab. Costs of third-party devices as well as their maintenance and support are cut to a minimum. In this way, the administration costs of the lab, including all the set-up and breakdown between classes, is significantly reduced.

In addition to classroom training, MIMIC lends itself to automated training so employees can learn independently of structured classes. This adds a flexibility that fits students' schedules, which classroom schedules often do not. With MIMIC, it is as if students have their own training lab! Moreover, independent, automated training for employees frees regular training class seats for revenue-generating customers.

Overall, with its ability to hold down hardware expenses, to enable training to be scheduled before devices are even on the shelves, and to reduce training lab administration, MIMIC provides the solution for today's employee training program.

### *Software Evaluation*

Until now, the only way for enterprises to evaluate network management applications – from element managers to frameworks to value-added applications – was to obtain a demo copy and use it on their network. Most enterprises, however, do not have extensive non-production networks on which to test these products, and they may be hesitant to install them on their production networks.

MIMIC and its SNMP agent recording and simulation capabilities change all that. MIMIC can record the enterprise's network, then use that recording as input for a simulation of the network. Management applications can then be run against MIMIC's "virtual network" – a network that is identical to the enterprise's production network. They are then free to evaluate the application. They can run tests using the simulated network, like disabling virtual devices to see how the management application reacts. They are also free to experiment with additions and changes to the network to test features like inventory management without worrying about the impact to the production network.

Using the applications in their duplicated network environment can give enterprises a personalized, accurate appraisal of the software. This provides an assurance that the software will perform to specifications. The enterprise user no longer has to guess whether or not an application will scale to meet their current and future needs. MIMIC allows them to create "what if" scenarios with their network configuration to evaluate the application in possible future scenarios. This allows them to know exactly what to expect from the application – and what not to expect.

### *Sales and Marketing Demos*

Effective sales demos of networking gear and network management software are difficult to produce. Networks are complicated, and most vendors cannot afford to set up a demo network in every sales office. A demo, however, represents the only way to show the complexities of software and to reassure customers that hardware is "real." Too often, a sales representative's only option is to fly their customers to the corporate demo facilities. While these facilities are very nice, the networks in them are extremely expensive to build and maintain, have to be shared among sales reps and others that need the facility, and force the customer to spend significantly more time than desired to get a demo. No one will ever know the number of sales that could have been made if demo networks had been available locally.

Until now, having a local demo network was a dream for most sales people. However, with the MIMIC SNMP agent simulation technology, virtual demo networks can be set up on a single workstation. With such a portable demo solution, demos can even be shown to customers right in their own offices.

In the past, software and hardware vendors that wanted to bring a network demo to a potential customer had to ship huge boxes of equipment to the demo site at a high cost. After the trauma of shipping, there was no guarantee that the devices would work, so smart vendors also sent spares. Set up was required by a technician, which meant taking them out of the field. The cost of all this was exorbitant, including shipping, devices and personnel time. Sometimes after all these efforts, the customer would end up canceling at the last minute.

Today, MIMIC can record a live network, then make the simulation of the network devices available during a demo. For device vendors, they need only show the client one real device, then use the simulation to demonstrate how that hardware scales and how its management application operates. For software vendors, the MIMIC simulated network allows potential customers to experience the capabilities of even the most sophisticated management applications, without the cost of purchasing and lugging around third-party networking gear.

In the past, many sales have been made at vendor showcases – special set-ups where customers were invited to view hardware and software solutions locally. Imagine the increased success of sales teams, each armed with their own personal demo system!

In addition to individual sales demos, MIMIC serves as an invaluable tool for trade shows. MIMIC's ability to record network scenarios and then to play them back really supports sales reps in explaining the benefits of their products. With MIMIC, reps are no longer limited to demonstrating their products on the few pieces of equipment available at the show. They can easily demonstrate even the scalability of their products through MIMIC's "network-in-a-box" capability. Demos sell, especially when vendors can properly demonstrate the extreme usefulness of their products through MIMIC.

### *Network Management Training Providers*

With network use exploding in every business – from LANs to WANs, from building to campus to global – the pressure is on for training classes to provide real-world experience in network management. Customers are increasingly looking for value-added resellers, third-party training companies and established educational institutions to complement the network management training provided by network hardware and network management software vendors.

Providing network management training, however, is a difficult task. Underlying the training of the software there needs to exist an extensive network of multi-vendor hardware that will give the student a real-world network management experience. How can a training provider offer such a costly network, satisfy their customers' training needs and still be profitable? By using MIMIC to provide the underlying network upon which network management training is based.

Through SNMP agent simulation, MIMIC provides a simulated network of devices to the network management application or platform the student is learning. Having a simulated underlying network with MIMIC not only reduces the capital expenses associated with training labs, it also reduces lab administration. Using simulated devices allows fast set-up and breakdown between classes to maximize the use of the training facility. In addition, the training scenarios and number and brands of devices used are unlimited – achievements that even the best-funded capital and administration budget cannot accomplish.

MIMIC also allows training providers to tailor courses to their individual customers. For instance, classes can be held for network operators on a simulation of their real-life network. This is possible through MIMIC's ability to record devices from existing networks, then use the captured information in simulations. Recording and simulating the actual network's devices bring the student's own network right into the classroom! This results in students who gain experience on their own networks in the lab, an experience that can be applied directly to their own operation.

Through use of MIMIC's agent simulation to provide virtual networks in the classroom, students can learn network operations techniques that they would not dare to try in their real network. In MIMIC's virtual lab, students are free to perform administrative functions that if performed incorrectly "at home" would bring down the network. Students can even be taught disaster recovery routines to prepare them for catastrophic events like site outages, major line cuts and natural disasters.

The bottom line is that using MIMIC to simulate network devices for the training lab enables training providers to train network management personnel in effective use of management applications and platforms. Courses no longer have to stop with reviews of software capabilities and basic labs. Students can truly experience managing a real network without the fear of harming that network. From daily monitoring duties to stressful network scenarios, students gain network management experience in a "safe" environment that cannot be harmed by a learner's mistakes. In addition to walking through the different features of their network management application or platform, students can learn real world skills, such as:

- Monitoring techniques and the individual organization's procedures;
- Troubleshooting of network problems;
- Planning for network upgrades; and,

- Inventorying the network.

### Management Service Providers

The basic tenant of network and systems management outsourcing is simple: turn over network and systems management to an organization that specializes in network management and focuses on nothing else. This provides personnel who are uniquely qualified to monitor and manage networks and have the know-how to meet the expectations of a service-level agreement. Customers that decide to outsource network and systems management want their environment to be monitored constantly and professionally. In addition, they do not want the hassle of daily operations and maintaining management personnel.

Theoretically, if an MSP or outsourcer adds clients to their roster, their economies of scale will allow a profit to be made in the venture. As clients are added, however, the complexity of the network and systems management knowledge necessary also increases along with the amount of customization necessary. Given this, how can MSPs and outsourcers effectively deal with the proliferation of networking devices? How can they keep employees' training up-to-date? How can they provide the internal tools that help meet service-level agreement clauses on network availability?

MIMIC's simulation capabilities for SNMP-based device recording and simulation provide one solution for dealing with the proliferation of network devices. Using MIMIC's ability to capture information on real networked devices (including servers), users then have access to that information in a multi-functional virtual lab. Engineers can determine the impact of additional hardware by creating "what if" scenarios using the simulations. Programmers have access to the real hardware information needed for developing custom applications. Support personnel can also use the simulations for troubleshooting remote problems, by recording the remote network and working on the problem at their local lab. This results in a reduction of travel time and the associated expenses. In addition, simulations can be used to train network operators, administrators, and technicians in a "safe" environment that cannot be harmed by a learner's mistakes or experimentation.

In addition, MIMIC allows MSPs and outsourcers to run disaster simulations without involving the actual, physical network. These disaster simulations provide an important way of assuring customers that their service-level agreements will be met, even in the event of a natural disaster, site outage or line cut. All these functions not only save time and money, but also make it possible to perform many tasks that are not feasible within the physical lab environment.

Overall, by using MIMIC, MSPs can support their customers with a higher level of efficiency and quality and get a much greater ROI with the virtual lab.

### Software Development

Software is pervasive in the networking industry — especially surrounding network management. Customers today require that network management applications be available for devices when they ship. Moreover, customers rely more heavily on their management tools to assure that their networks are available.

In the software development environment, acquiring networking devices creates a constant, unnecessary and time-consuming struggle. Device vendors never seem to be able to meet software developers' needs for devices. It seems there is an unquenchable thirst for devices… from the developers that design and program the device management applications to the QA personnel in acceptance labs. Pre-production devices are very costly and almost non-existent for the software team. In software development organizations that do not manufacture their own hardware, the hardware situation is even bleaker. Every piece of third-party equipment must be purchased with hard-won budget money. In addition, the time to research, purchase, install, inventory, and depreciate consumes time that could be better spent developing software.

By using MIMIC, software organizations can overcome the hardware obstacle, and device companies can assure that software applications are available when the hardware hits the streets. MIMIC has the ability to simulate SNMP agents, thus making virtual devices available in development labs. As a matter of fact, MIMIC can even make some labs obsolete by providing each developer a private, virtual lab. Imagine not having the overhead and administrative headaches of development labs – and the scheduling nightmares they cause. MIMIC can eliminate all these issues while providing a trusted tool with which to develop quality software.

Developers can, therefore, truly engineer scalability into their products and test those designs against MIMIC's virtual devices. In addition to scalability, developers can exercise even the most sophisticated network management products – from platforms to filtering tools to reporting applications. Developers can even capture real networks with MIMIC's recording capability, then use those recordings as simulations against which to test their applications.

With all of the advantages of MIMIC in software development, like the shortened software development cycle, reduced overhead and fewer political battles over hardware, software developers can focus on what they do best – developing more management applications.

### *Partner Support*

Any company that develops network management applications — whether the products are element managers for their hardware, platforms and frameworks or advanced applications like reporting and alarm suppression — finds that they need a variety of industry partners. These partnerships validate the interoperability with each other for the customer. Due to the nature of implementing network management, it is as if there exists a giant grid of interdependencies within the network management industry. Framework and platform vendors need support from device and application providers, device vendors need support from framework and platform providers, and application vendors need support from framework and platform vendors as well as device vendors.

Partnerships are good. They increase customer confidence by showing that vendors are working together. However, when the reality of supporting partners hits, how can a company support so many necessary partnerships? In this role, device vendors are called upon to make their devices available for testing, and software providers are called upon to provide certification labs based on networks. All of this creates a great expense, not to mention the scheduling constraints inherent in running a certification lab.

With the use of MIMIC SNMP agent recording and simulation capabilities, many of these partnership costs can be reduced. MIMIC can record certification lab networks or even individual devices. MIMIC then uses those recordings as the basis for SNMP simulations that can be used in partner programs to verify the interoperability of devices and applications.

Making the MIMIC simulations available to partners lowers the cost of the partnership program and reduces the time and expense of partners visiting certification facilities. Once the network has been recorded, each partner can receive an identical copy – changes in the network will not impact certification results. Device vendors never have to worry again about allocating brand new products, which are hard to come by, to the software partner program.

By providing virtual devices and networks to partners instead of shipping out prototype and tracking prototype products or maintaining certification labs, MIMIC provides increased savings and control. MIMIC simplifies and reduces the cost of partnership programs and improves partner relationships.

### *Device Vendors*

One of the biggest complaints of networking hardware customers is that the network management software is never ready when the hardware is released. Executives of hardware companies constantly come under fire for this during user group meetings. Hardware manufacturers are constantly placed in a difficult situation, since the competitive pressure in the constantly evolving marketplace is fierce. New standards are constantly emerging, and old ones are being updated. Emerging technology leapfrogs available products every 18 months – sometimes even less!

Investors constantly scrutinize the bottom line, looking for hardware manufacturers to squeeze as much profit as possible from an increasingly crowded marketplace. In addition, customers have learned to expect twice the power at half the price every year. Given this, how can a manufacturer increase profits? By following the simple, unyielding accounting truths: increase revenue or cut costs.

When faced with this choice, many manufacturers have turned to MIMIC. SNMP agent simulation can be used in many areas in device manufacturers, and it is especially effective in controlling costs in network management software development while helping to move new hardware to the shipping/revenue phase quickly.

SNMP agent simulation replaces actual hardware product use in development labs, test labs and training facilities. With MIMIC substituting for hardware devices in the software development process, the need for pre-release devices is minimized – and every manufacturer knows that pre-release devices are costly and cannot be refurbished for later sale. Even when devices start coming off the manufacturing line, vendors know the pain of the constant pull between allocating devices for development and testing or making those devices available to fill backorders and generate much-needed revenue. With MIMIC, these conflicts are erased. Devices are available for customer orders, with network management applications available earlier in the cycle.

MIMIC helps reduce costs and improves deployment in many areas. The resulting product will have higher customer satisfaction, because it was thoroughly tested in all types of scenarios. In addition, it allows for software support to be available for network devices when they reach the market.

### *QA and Testing*

Software testing is a thankless job. It always comes at the tail end of the development cycle, and the pressure to hurry and release the product is phenomenal. Of course, the development cycle includes many types of testing. Types of testing that require a lab with working networks include unit/module testing to spec, integration testing, acceptance testing and documentation testing. In larger organizations, each type of testing requires its own testing labs. The personnel that use these labs have the responsibility for assuring that software works in a variety of network environments with multi-vendor hardware.

"Real engineers," who develop the product, often look down on testing. Due to this, testing labs are sometimes not as well endowed with devices on which to test the network management applications. In addition, since development comes before testing in each phase, development labs usually receive priority when it comes to new equipment. Too often, testers must compete against developers for the limited resources required for building lab networks. However, the testing department ordinarily receives the blame if there is even one bug in the software, in spite of who made the decision to ship.

How can companies assure the quality of their network management software products without spending all their profits on third-party devices? By investing in MIMIC. This allows the creation of virtual networks and even provides each tester with a virtual lab. These "private labs" allow testers to concentrate on predicting what problems will occur, without interference from others who would normally share a physical lab. With MIMIC in the testing lab, management can eliminate the turf wars and ensure productivity. MIMIC can even record actual network configurations and bring them right into the lab, as part of the test plan. MIMIC allows testers to perform complete testing in all types of scenarios, providing more thorough testing. Moreover, MIMIC's scalable scenarios allow testing of even extreme scenarios that would be virtually impossible in a physical lab. In addition, MIMIC makes regression tests a snap, because MIMIC can record test scenarios and replay them. Scenarios can be run forward, backward, fast forward and fast backward at will – like a VCR! Imagine the time this would save in the testing procedure!

With MIMIC, testing can proceed faster and in more depth. Companies can have higher confidence in the level of software testing, and software products can be released to customers more quickly. Winning the time to market battle with the competition is more important than the internal developer vs. tester battle!

### *Certification*

There are several areas where vendors in the network management industry may need to provide certification programs, including:

1) Certifying that device management partner applications integrate with platforms, frameworks or advanced applications;
2) Certifying that management applications like trouble ticketing and policy management integrate with platforms and frameworks; and,
3) Certifying for customers and partners that applications run properly on particular network configurations.

Although certification programs are valuable –assuring customers of interoperability – these programs are time-consuming and expensive to implement and do not produce revenue. Certification programs require their own, individual labs with dedicated networks. Due to the nature of certification and its significance to customers and partners, the underlying networks should not be used for other purposes to avoid the appearance of contamination – the results of a certification need to be above question.

MIMIC's SNMP agent recording and simulation capabilities can replace the physical networks now used in certification labs. MIMIC can record an existing network's devices, then use simulations of those devices to form a virtual certification lab. This eliminates the time and expense of creating a lab from scratch and purchasing the necessary hardware devices. In addition, copies of the "virtual lab" with testing instructions can be sent to companies seeking certification. They can use MIMIC's virtual lab in their certification preparations and even run self-certifications, returning the results to the certifying company. For companies seeking certification, this greatly simplifies the certification process and reduces costs, like travel, involved in seeking certification. In addition, the certification test can be run when it is convenient because the virtual certification lab is always available!

MIMIC's ability to record existing networks is also valuable in certifying to customers that network management applications will operate properly in the customer's actual network environment. MIMIC can record the customer's network. Running the application on the simulated network shows potential customers how a product operates in their environment without installing the management application on the physical network. This assures the customer of proper operation in their environment before purchasing the application.

Whether setting up a new certification program or maintaining an existing one, MIMIC's SNMP agent recording and simulation capabilities save time and money, while adding flexibility in certification testing previously unavailable.

### Customer Support

Software support is a tricky business… often, it is difficult to understand what exactly is happening in a customer's network in order to identify the root of the problem. In addition, with networks and the applications both becoming more sophisticated, identifying the root has also become more complicated than ever. Many support calls sound like a 20 Questions Game, trying to gain information on the customer's network: "What devices have you added recently? Has your network configuration changed? How many routers do you have and where are they located?" And so on. During the inquisition, the customer often feels that they are being blamed for the cause of the software malfunction. It is a time-consuming ordeal that must be endured.

Many times, support personnel have to visit the network in person. This is a huge expense, both in travel budget and personnel time, but identifying the root of a problem is generally easier when done with direct network access.

Fortunately, MIMIC and its SNMP agent recording and simulation capabilities provide a solution that can assist support personnel in determining root causes and eliminate their travel time. Using MIMIC to record the customer's network devices, the support person then has access to a simulation of the customer's network to troubleshoot. They can see for themselves exactly how the software interacts with the network and where the problem and its solution lie.

Reproducing the problem represents one of the most time-consuming parts of diagnosing problems. This often requires setting up traffic generators and network analyzers. With MIMIC, this is no longer necessary. MIMIC's ability to record a network allows technicians to "replay" the scenario and to recreate it virtually – without disturbing the network and setting up physical scenarios. Actual scenarios can be run forward, backward, fast forward and fast backward at will. Imagine the time this would save in diagnosing problems, especially with problems that only appear at certain intervals – for example, every 30 days. With MIMIC, there is no need to wait for the problem to reoccur. Technicians simply fast forward 30 days, and the problem is there for them to work on!

With MIMIC, software problems can be diagnosed more quickly. In addition, by avoiding at least part of the inquisition, customer satisfaction is bound to improve.

### Customer Training

Customer training provides one of the first opportunities for a company to solidify a relationship with a client and to make a good initial impression. Students will judge a company and its products by the quality of training they receive as well as the quality of the educational facilities and tools. They will take those opinions back into the workplace to work for or against the vendor. Students attend training to learn about new devices being added to their networks, as part of their professional development, and to learn new network management tools. Training is generally offered either at the vendor's training center or on-site, at the customer's location.

In the network industry today, training is in heavy demand due to the proliferation and sophistication of devices and networks as well as the variety of network management applications. Training is not only provided by hardware and software vendors, it is also offered by value-added resellers, third-party network service organizations and traditional educational outlets like universities, colleges, technical schools.

The foundation for most training in the network industry is a training network that allows students hands on time, especially with the network management software. Providing a network for customer training labs, especially multi-vendor device networks necessary to teach fully the capabilities of network management platforms and applications, is a costly and time-consuming undertaking. Devices are constantly out of date, and different lab exercises require different configurations. How can a training lab meet the expectations of the students for up-to-date equipment and meaningful, real-life lab exercises?

MIMIC's SNMP agent simulation capabilities provide virtual devices that can be used to set up training lab networks. These virtual lab networks can become as extensive and complex as the trainer desires, which allows them to teach fully the capabilities of the element manager or NMS application. Network management platforms and today's emerging point solutions have extensive capabilities that scale for use by enterprise customers. Having access to an unlimited number of virtual networking devices allows the trainer to represent properly these capabilities in labs and demonstrations. In addition, with MIMIC, students have the opportunity to practice "real world" scenarios – both positive and negative – that would be impossible with a physical network.

On-site training is usually cumbersome and limited by a few available devices. If the trainer is given access to the customer's network, that access is restricted for security and "safety" reasons. No company wants students experiencing network management first-hand on the production network! By using MIMIC, however, the trainer can capture a real-life network through MIMIC's recording capabilities, then use that network in a simulation for students' labs. MIMIC can even capture a customer's network so students can train directly on a simulation of the "real thing."

With MMIC, hardware vendors can provide training on new devices earlier in the product cycle, without having to wait for the training lab's manufacturing allocation. Imagine being able to provide courses for customers, even before their products are shipped! Moreover, this allows the initial production to be earmarked for customer shipments, instead of for use in labs.

Providing customer training that makes use of MIMIC's SNMP agent simulation capabilities substantially reduces training lab expenses. Costs of network devices as well as their maintenance and support are reduced to a minimum. In addition, administration costs of the training lab, including all the set-up and breakdown between classes, is significantly reduced. Vendors report that students are happy with the training results using MIMIC – and happy students lead to higher overall customer satisfaction and repeat business.

## MIMIC'S BENEFITS

### *More productive network management staff*

Generally, there are multiple teams with different needs for developing products sharing the same lab. Testers may require a sizeable network, for example, to test the scalability of the application. A developer implementing policy scripts may need to reproduce fault conditions to ensure proper operation. This time-sharing in the same lab affects development schedules. With MIMIC, individual developers can have their own networks on their own machines all the time. This results in significantly faster production schedules. Technical staff can easily manage and configure an entire "virtual" enterprise network, safely putting complex network management products through their paces without impacting anyone. Ongoing products can be customized to site-specific policies.

### *Greater revenue with lower cost-of-sales*

MIMIC reduces the initial capital costs of the lab by factors of 10 to 1,000, since there is no need to buy the variety and quantity of hardware from different vendors. Less equipment also means less real estate, infrastructure, support staff and the associated costs.

### *Accelerated product time-to-market*

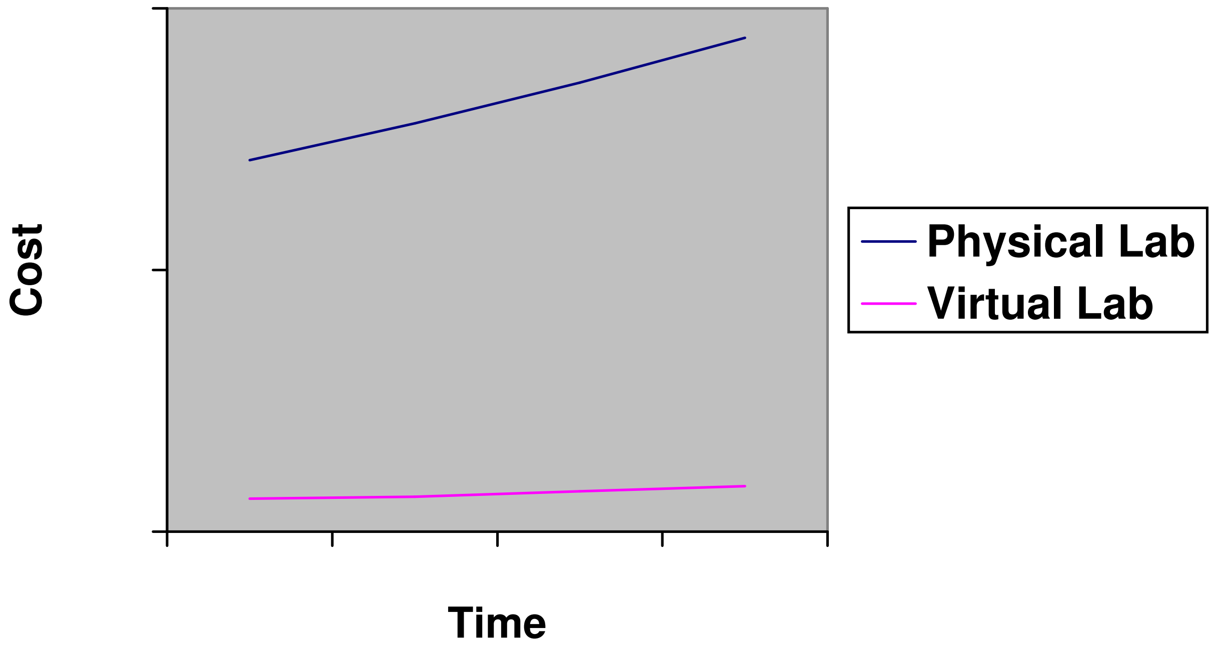
Simulation of device prototypes during the development phase facilitates parallel development and lowers time-to-market. Hardware and software developers can all work together without needing to wait for the other group to complete development. If the application needs to support third-party devices, development and test engineers will not need to wait for the budgeting, purchasing and shipping of the equipment.

### *Lower customer support costs*

From development to QA to customer support, MIMIC enables greater product quality throughout the life cycle. This translates into reduced customer support calls and faster customer service. Moreover, customer support spends a significant portion of its efforts in recreating the customer's problem at the vendor lab. MIMIC easily captures the exact customer configuration for duplication at the vendor's facility, resulting in speedier problem isolation and diagnosis.

### *More reliable network management products*

MIMIC simulates the complexity and scope of an enterprise network to enable faster and more complete QA testing prior to product release. The determinism of MIMIC simulations enables formalized regression testing. Negative conditions, which happen very infrequently, are hard to recreate. With MIMIC, even pathological conditions are easily reproduced, since MIMIC gives control over every single MIB object instance of every agent at any point in time. Instead of using traffic generators, call generators or any other physical devices, MIMIC supplies a batch-processing environment that can run unattended.



***Greater ROI for network management products***

Investing in MIMIC instead of hardware for 100 managed devices can provide investment savings for each area as follows: capital resources — 98%, engineering — 96% and operations — 64%.

## CONCLUSION

With today's tighter profit margins and an expectation from investors for greater return on their investments, the costs, both administrative and financial, associated with physical labs can be prohibitive. Gambit Communications' MIMIC SNMP Agent Simulator can greatly reduce this burden, and in some cases, it can even completely eliminate the need for a physical lab.

# APPENDIX: CASE STUDIES

## *MIMIC Powers APC's Quest for Scalability*

When APC needed assurance of software scalability, they turned to Gambit's MIMIC SNMP Agent Simulation Tool. APC, who develops the world's most advanced power management software for its complete line of power protection equipment, was tasked by their customers to provide an application with inventory and status insight into enterprise-wide installations of APC's UPS systems. As the developers began working on this unique application, they realized that the testing required to validate the customers' scalability needs would be a challenge — a unique test bed for scalability would need to be built. In order to assure that the new PowerChute Inventory Manager could find the 1000s of APC devices typically installed across a customer's enterprise, engineers would need to spend massive amounts of time and capital to build a hardware lab just for testing the scalability of the new software. The undertaking was, frankly, cost prohibitive.

In searching for scalability testing alternatives, APC decided to use an SNMP Agent Simulator — a product that could simulate their devices and allow the use of those virtual devices in virtual test beds. For numerous reasons, APC chose Gambit's MIMIC for the job.

"We looked at other simulators, but MIMIC was easier to use. It also supports Linux, which we use in our development environment. Basically, our biggest requirement was scalability, and MIMIC was the only product on the market that fit the bill," said Brad Hammond, Software Program Manager, APC.

APC's developers used MIMIC to "record" the device MIBs for the APC product set, including the APC SNMP Software Agent and the Web/SNMP Management Card — a card that makes managing APC UPSs a snap. The web card provides APC's customers the ability to manage, configure and control their power protection devices via SNMP, Telnet or even HTTP. MIMIC was then used to simulate the devices and Web Cards. Simulation scenarios were created with 1000's of devices — just like a customer's enterprise – and the claim of managing 10,000 devices was substantiated.

In the later development phases — integration, alpha test, and beta test — MIMIC was used by the development team (both by developers and QA engineers) to assure that the scalability of the new product held true through each phase. In many companies, scalability testing is often put off until the end of development cycles, if it is done at all. Many companies test scalability when their products are installed in a customer's network — not a particularly good time to uncover issues! With MIMIC, APC's engineers had the assurance early in the development cycle that their PowerChute Inventory Manager software would meet their customers' scalability requirements.

APC attributes huge cost savings to MIMC. The entire cost of building a physical scalability lab was avoided — including the capital expense and administration costs. In addition, APC did not have to assign development resources to creating scalability tests. As a result, APC's developers were able to focus on the PowerChute Inventory Manager's functionality, and insure it worked to specification and was of the highest quality.

### *MIMIC Helps InteQ Manage*

*InteQ's InfraWatch™ is a management service that provides proactive monitoring, notification and Web-based reporting on the health of complex IT and Internet infrastructures. Charged with servicing enterprises whose infrastructures are comprised of all types of networking gear, servers, databases and applications from vendors around the world, how does InteQ assure customer satisfaction given this heterogeneous mix? By simulating its management services before implementing them.*

When you're the first Management Service Provider (MSP) on the market, you have to stay way ahead of the competition in terms of service offerings. In the MSP space, the more customers you take on, the more scalable and diverse your service has to be. You are expected to manage any brand of server or networking device, as well as the mission-critical applications that fuel daily business operations. So, how do you cope with the needs associated with managing large enterprise networks? One solution for InteQ is the MIMIC™ Simulator and its SNMP agent simulation capabilities. By using the MIMIC Simulator before monitoring services are used in production, InteQ assures excellence in management and, therefore, customer satisfaction.

When InteQ decided to use a simulation tool, the engineers conducted an exhaustive search and test of all available alternatives. At the end of this rigorous exercise, they determined that the MIMIC Simulator was the best solution for many reasons, including:

- MIMIC was the only simulation tool that had the scalability InteQ required for simulating tens of 1000s of nodes from multiple enterprise customer environments.
- MIMIC's extensive library supports virtually any SNMP-manageable object. The library is updated frequently, and there is a mechanism to easily add devices that are not in the library.
- Only MIMIC has the capability to manipulate parameters and simulate different network conditions.
- MIMIC runs on many platforms, including Linux and Solaris, which is very important to InteQ.

"In addition to these technical reasons," said Jay Martin, Director of Network Infrastructure Engineering at InteQ, "the Gambit Communications personnel consistently exhibit a can do attitude given our unique business model. Everyone from the sales team to the technical staff was able to understand our requirements and package a solution that has really worked quite well for us. They really took the time to understand our needs and go the extra mile."

InteQ is planning to implement use of MIMIC in both its R&D and operations areas. In R&D, MIMIC is used in the development of future enhancements to InteQ's subscription-based services. These services include InfraWatch™, InfraStream™ for data correlation and analysis, as well as a reporting portal called InfraPortal™. MIMIC's simulation capabilities are used to assure the scalability and reliability of enhancements to these services before they are put into production, managing customers' IT environments.

"Our business model is based on a one-to-many model, which means that we must be able to provide 24x7 visibility to hundreds of customers and thousands of objects from a few Monitoring Points-Of-Presence™ (M-POPs™)," continued Martin. *"MIMIC was the only way to test this level of scalability for our services without bringing in dozens and dozens of servers and network* *devices."* With MIMIC, InteQ can set up virtual customer labs that simulate real IT environments. By using virtual customer labs for test and development, InteQ will avoid the capital cost of setting up a massive physical lab, as well as the administration headaches associated with managing such labs. MIMIC allows InteQ's engineers to get right to work on designing and testing new enhancements instead of designing and building physical test labs that are expensive, resource intensive and become obsolete quickly.

*"With MIMIC, InteQ's engineers are able to perform real-world simulations to test the performance, reliability, and look and feel of management services before they're put into production," said Stephen Elliot, E-Services Manager at InteQ.* In addition, MIMIC easily allows InteQ's engineers to develop custom management for their clients. When customers request the management of new devices, InteQ will be able to remove the guesswork from this process and meet the client's needs right from the start. MIMIC allows InteQ to generate a list of events that the new device can generate, then review that list with the client to prioritize importance and set thresholds that meet the client's individual needs. For many service providers, this process is fraught with guesswork after management begins, ending with frustration on the client side as the process draws out and useless events are generated.

In addition to R&D, InteQ's operations personnel benefit from MIMIC's simulation capabilities. InteQ has a 24x7 NOC that responds to infrastructure issues at clients' sites. MIMIC can be used to train operations personnel when new applications and enhancements are made, before they are put into production. Training in a simulated environment allows operators the freedom to experiment with and learn new features, knowing that they cannot endanger the virtual customer network on which they are learning. In this way, operators can experience new alarms and events and be prepared for dealing with them when they appear while managing client networks.

With the help of MIMIC's simulation capabilities, InteQ plans to continue to lead the MSP marketplace in introducing new and innovative management services. "Our company background in IT service management consulting and management services gives us the knowledge base to innovate and attract mid-sized and large enterprises to our service offerings," summed up Elliot. "MIMIC allows us to quickly implement those innovations and meet the growing customer demand for IT management services."

### *Avaya Cuts Demo Costs with MIMIC™ Simulation Tool*

The options for demonstrating networking hardware and the sophisticated software necessary to manage it are limited. Should vendors rent a truck, load it up with equipment and cabling and take it to the customer site? Where would they set it up once they get it there? Should they try to demo the software on the customer's network? Would the customer allow access to the network for that? What types of unforeseen obstacles – potentially ruining the demo – would be encountered when installing software on a network for the first time? Or should vendors incur the cost to rent a conference room near the customer and spend hours setting up a system, only to have the customer reschedule? Or should they fly entourages of potential clients to a corporate demo center, only to find that one additional person who is key to the decision cycle is not included in the party?

These options consume time and money – not to mention the peril to the potential sale – requiring extensive personnel effort and capital resources. Due to these factors, actual demos of sophisticated networking equipment and network management software are often limited to "serious" customers who warrant the expenditure.

To solve this sales conundrum, Avaya decided to provide laptop-based demos of the complex software and hardware to enable sales force efficiency. Avaya tapped MIMIC, an SNMP agent simulation tool by Gambit Communications, for use in their CajunView Suite laptop demo.

CajunView provides a suite of SNMP-based applications for managing complex enterprise networks more easily. With this product, enterprises using Avaya Cajun Campus products can configure, monitor and control these devices using a single, integrated suite of applications — everything from device configuration to advanced switch monitoring and VLAN management.

Avaya's CajunView engineers were already using MIMIC to provide simulations of Cajun devices in the test and development cycle, and had seen how it could solve the sales demo situation. MIMIC provided the ability to demonstrate the CajunView's unique switched management, without building costly demo facilities or traveling shows.

Today, the sales force – which is charged with selling both CajunView and the Cajun switch line – can demo CajunView's switched monitoring features right from their laptops. This demo mobility increases the number of potential customers that can see CajunView during the decision process, and may eventually lead to shorter sales cycles.

"With MIMIC simulating the hardware, the sales force can show CajunView exactly as they would on a live network," said Bob Shaw, Marketing Engineer of Avaya. "Customers can see how CajunView handles alarms, how easily devices are diagnosed and configured, and how the different switched network segments are monitored simultaneously. And MIMIC is totally transparent to the sales force, so there's no additional training time involved."

Based on the SMON standard, which extends the RMON management standard to switched networks, Avaya's SMON Master portion of CajunView provides simultaneous management of all switched segments in a network. Many offerings in the marketplace only allow the monitoring of one segment at a time, which makes CajunView an indispensable real-time management tool. MIMIC's switch simulations allow this multi-segment management capability to be accurately and effectively demonstrated to customers. With MIMIC's simulations, there is no difference between running a demo with a real device or a simulated device.

MIMIC's demo scenarios are often more useful than with real networks, because many scenarios are difficult or impossible to create with real networks. For example, on a real network it is hard to create broadcast storms that suddenly grow disproportionately large, or malfunctioning NICs generating large CRC errors, or an Uplink that is causing an overload/congestion situation. MIMIC easily simulates and reproduces these scenarios. Avaya's sales force can take advantage of this capability to show how SMON Master detects and resolves all these typical problem scenarios.

For the Avaya sales team, MIMIC has eliminated the expense of maintaining additional demo hardware and live demo facilities, as well as the time-consuming coordination of either setting up demos at customer sites or coordinating customer visits to demo centers. Eliminating the shipping of hardware for demos alone represents significant savings.

In addition, the sales team never needs to worry about whether demo equipment and facilities will be available – the demo capability on their laptop exactly duplicates CajunView's functionality in a live network. From facility costs to equipment capital budgets to shipping costs and personnel administration time, using MIMIC's simulation capabilities to automate the CajunView demo will create savings throughout Avaya's sales and marketing organizations.

## GLOSSARY

**ASP** (application service provider) — a company that provides applications to customers over the Internet.

**ATM (asynchronous transfer mode)** — a packet transmission standard that uses fixed-size packets.

**CLNS** (connectionless network service) — an OSI packet-switched network where each data packet is independent and contains complete address and control information.

**DOCSIS** (data-over-cable service interface specifications) — DOCSIS defines the protocol for exchanging upstream and downstream information over cable.

**GUI** (graphical user interface) — a computer application interface that provides users information and choices in a graphical environment as opposed to a strictly text-based interface.

**IOS®** (internetwork operating system) — Cisco Systems' IOS® is software that runs on vendors' routers.

**ISP** (internet service provider) — a company that provides Internet connections and services to customers.

**LAN** (local area network) — a group of computers and network devices that generally share a local server (or servers) within a small geographical location, i.e. within a building, etc.

**MIB** (management information base) — a database that contains information about a manageable network device. This information can be accessed and managed using SNMP. There are both general MIBs that provide information about a general type of network device (such as routers, etc.) and private MIBs that contain proprietary information about a specific device (such as a specific Cisco router model).

**MSP** (management service provider) — a company that provides network management services for clients usually from a remote location.

**NOC** (network operations center) — an operations center within an organization where the network is supervised, managed and maintained.

**OSI** (open system interconnection) — a standard description for handling and transmitting messages between points on a telecommunications network

**packet** — a unit of information that contains data including control information.

**RMON** (remote monitoring MIB) — provides detailed information about local network traffic conditions

**RMON2** (remote monitoring MIB 2) — provides a standard method for identifying application flow within the network as well as statistics about the usage of each application and the identity of who is using an individual application.

**TCP/IP** (transmission control protocol/internet protocol) — the basic Internet protocol.

**WAN** (wide area network) — a group of computers and network devices that generally share a server (or servers) across various geographical locations.

## THE MIMIC PRODUCT SUITE

The three components of the MIMIC product suite work together to provide a complete SNMP-based network simulation capability on a single computer.

### *MIMIC Simulator*

The MIMIC SNMP Agent Simulator allows for the simulation of an entire enterprise network on one Intel®-based PC or Sun® Microsystems Sparc™. With support for any SNMP-based device, a variety of device configurations can be performed with a management application.

Configurations are completely run-time customizable, both on an individual and collective basis. Since MIMIC responds to SNMP v1, v2 and v3 queries on any of its configured IP addresses, it looks to the Network Management Application as if it is talking to actual devices.

### *MIMIC Compiler*

The MIMIC Compiler allows users to import any SMI-compliant MIB and extend the set of defined devices to support proprietary or unique equipment. Vendors use the Compiler to import definitions of new devices in the prototype development phase.

With an intuitive graphical interface or a powerful, flexible scripting language, users can further customize any device in the MIMIC library to simulate unique network behavior.

### *MIMIC Recorder*

The MIMIC Recorder enables users to automatically simulate the behavior of actual devices on a network by capturing a "snapshot" of the device MIB in actual operation. The snapshot can then be easily replayed by the Simulator to simulate an entire network with minimal user effort.

Any number of target devices can be recorded in parallel. Any subset of the device MIB objects can be recorded. For example, if a problem investigation focuses on a small part of the MIB, snapshots can be taken of the relevant MIB subtrees. The recording can be saved in a format for future editing, annotation. Recordings can be exchanged via e-mail and source code-controlled.

### *MIMIC Device Library*

MIMIC ships with a large library of simulated devices, networks and pre-compiled MIBs from the leading networking companies.

MIMIC standard package includes the following:

### *Tools*

- **MIMICView** - User-friendly GUI to manipulate the simulations
- **MIMIC Simulator** - allows you to simulate an enterprise network on a workstation
- **MIMIC Recorder** - captures a "snapshot" of the device/network and creates the simulations
- **MIMIC Compiler** - Compiles any SMI-based MIB
- **MIMIC Shell** - Command-line interface

### *Wizards*

MIMIC Wizards give a user-friendly way to compile, record and simulate huge networks.

- **Topology Wizard** - Customizes different network topologies

- **MIB Wizard** - Allows importing new MIBs
- **Discovery Wizard** - Records large networks
- **Simulation Wizard** - Helps creating simulations for devices under development

### *Libraries*

- **Device Library**
- **Networks Library**
- **MIB Library**
- **Script Library**

### *Platforms*

MIMIC supports Windows®, Solaris™ and Linux™ operating environments**.**