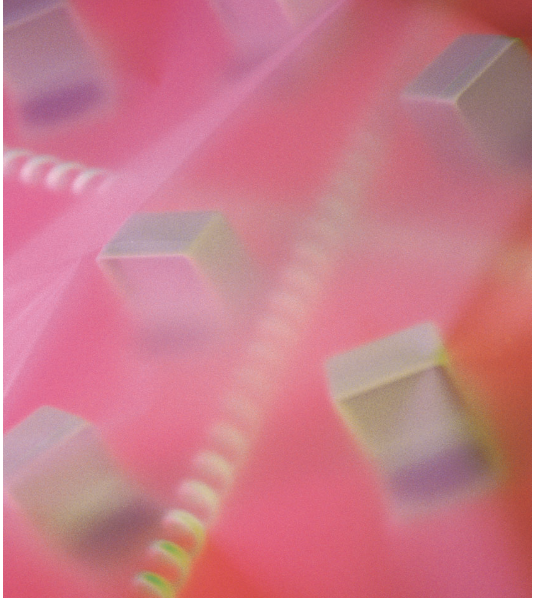


Input from network operators reveals that current solutions are based on faulty principles. Highly automated service-centric solutions are needed.

Stefan Wallin and Viktor Leijon

Rethinking Network Management Solutions

As with any technology, it's important to focus management solutions on the users, even when the users are those providing a service. In that broader context, network management has three types of "users": *network operators*, which must earn money on their services, *network service users* (business and consumer), who pay for using services, and *network administrators*, who staff the network operations center. All three user types benefit from a well-thought-out management solution: operators increase their profits, service users get better service, and administrators streamline their workload.

In short, the right network management solutions empower network operators to provide new services, maintain service quality, and manage billing and usage (TeleManagement Forum enhanced Telecom Operations Map, http://www.tmforum.org/browse.aspx?catID=1647). By its nature, network management is a hierarchical, centralized function that puts the operator in control; therefore it makes sense to provide a centralized network management solution. Operators are under pressure to reduce network operating costs *and* provide new services at an increasing speed. These two requirements highlight the need for an effective, automated, network-management solution.

To explore such a solution, we interviewed people in charge of large telecom network management centers and identified six challenges facing big telecom operators:

- *Excessive alarms:* A medium-sized operations center receives 100,000 to 1,000,000 alarms per day.
- *Constant changes:* New or upgraded devices and new services launch frequently.
- *Complex services structure:* Services are vital for business and customer interaction, but they are not really managed.
- *Customer interaction:* Operators must handle customer complaints, customer care, selling services and service-level agreements (SLAs).
- *Cuts in operations costs:* A small team must run a large, multifaceted network.
- *Difficult interface integration:* Diverse equipment and support systems make managing interface integration a challenge.

We then considered strategies for tackling each of these challenges and determined several best practices.

Excessive alarms

The bulk of network administrators' daily work involves alarms. Unfortunately, the large number of alarms indicates that the systems produce many irrelevant and noncorrelated alarms, making it hard to understand the true state of problems in the network.

Today's alarms are more or less raw alarms from the different equipment and vendor-specific management systems. Operators must establish an efficient organization to handle the alarms, a process that typically follows three steps:

1520-9202/06/$20.00 © 2006 IEEE

- The first-line organization performs three tasks: check for alarms that indicate the same problem, group the alarms and attach them to a trouble ticket, and distribute problem information to affected parties, such as SLA customers and customer care.
- If it's a simple problem, the first line resolves it and closes the ticket.
- If it's a complex problem, the first line dispatches it to the second- and third-line organizations. This might involve equipment vendors or operator staff in the field who might perform onsite management, card replacement, and so on.

The ever-increasing number of systems and services increases the number of alarms. Still, operators can't afford to employ additional people to handle the alarm lists, and automatic solutions are limited. Automatic trouble ticketing, for example, manages the workflow from problem identification to problem solution, but its usefulness doesn't extend to prioritizing the alarm's importance. Such knowledge is critical because an alarm's context determines if it affects services, customer SLAs, and the affected equipment's state. The resource emitting the alarm typically doesn't know the context, so the network-management system must supply it through alarm filtering and correlation.

The dynamic nature of networks and services puts increasing focus on change management.

Alarm-correlation projects are complex and not particularly successful. First, alarm quality is insufficient. The information carried in the alarm messages is not good enough to feed automatic-correlation engines. Second, the network lacks an overall network topology. In many cases, alarms are symptoms of a failure somewhere in the network. When a network doesn't have a model or system in place that keeps track of all of its resources and their relationships, it's difficult to implement rules that can deduce a fault's root cause. Third, correlation knowledge is spread across the organization and over several domain experts. This makes the organization too dependent on individuals and hinders centralized efforts. Finally, operators fail to use important alarm contexts such as trouble ticketing, inventory, customer care, and SLA management systems. Trying to correlate alarms using only the alarm information will lead to only minor improvements.

The operators we interviewed also noted the high cost of integrating alarm interfaces from equipment into the overall management system. In typical Simple Network Management Protocol (SNMP) agents, every box has its own specific mechanisms for alarms. The Disman working group at IETF has tried to resolve it by defining a standard MIB for alarms, the Alarm Management Information Base (IETF RFC 3877, S. Chisholm and D. Romascanu, Sept. 2004; http://www.rfc-editor.org/rfc/rfc3877.txt). However, we have not seen equipment vendors moving in this direction for their SNMP interfaces. Alarm integration at operators are still equipment specific and time-consuming.

Another organizational issue is managing the knowledge of how to resolve problems. Alarm texts from network equipment are usually cryptic, without any hints of how to fix the problem. Thus, operators incur steep training and productivity costs when hiring new people or introducing new equipment types.

Constant change

Networks change. Network elements are upgraded, new services launch, and customers come and go. These daily changes are a challenge for operators and network management solutions. Few operators have a fully controlled or automated process for handling these changes. Moreover, the network organizations are introducing critical equipment into the network without informing the network administrators. Surprises occur in the monitoring activities when unknown alarms and equipment suddenly appear. SLAs and business-critical services are sold to enterprise customers but without corresponding support in the management solution to actually monitor the specific SLA or customer.

The dynamic nature of networks and services puts increasing focus on change management. The expected time for changes has dropped from months to hours. We see operators and organizations realizing this and trying to reuse the change management process from the Information Technology Infrastructure Library framework (http://www.itil.co.uk/), a set of best practices drawn from public and private sectors worldwide. Change management's goal is to ensure that standardized methods and procedures are used to efficiently and promptly handle all changes to minimize its impact on service quality, consequently improving the organization's daily operations.

Complex service structures

Services' complex structure is an underlying problem in network management solutions, according to one operator we interviewed. Often operators do not have true visibility of services across processes and systems. There is a discrepancy between how customer care manages service problems and how the assurance and repair organization manages physical resources.

With those background problems, operators are looking for service management solutions or even SLA management solutions. Generally speaking, the industry must solve several underlying problems before successfully deploying such systems:

- *Topology management*: network topology, service topology, and the mapping between these.
- *Service management:* formal but dynamic management of services, SLAs, and customers, across all processes and systems.
- *Service centric integration and modeling:* use of service types and instances as keys in information systems, customer care systems, fault management systems, and so on.

Customer interaction

Being an operator in the current telecom environment is far from what it was 10 years ago. Customers now compare on the open market such factors as quality, service, and price. Therefore, operators must stay in close contact with customers, keeping them apprised of service status, including problem resolution, and providing them with clear, easily interpreted bills. This communication level requires a network management solution that can map resources and alarms to services and problems in a way that customer care and the customer can understand. Operators must prioritize work on the basis of service and customer priority, yet there is a big gap between customer care and the corresponding technical network management organization.

Pressure to cut operations costs

Operators are trying to cut operational expenses for both operating the network and introducing new services and equipment. Previously, it was acceptable to spend a couple of months integrating new telecom equipment. Now, any integration must be complete within a week. The number of people managing the provisioning, assurance, and billing solutions is minimal. To cut costs, many operators also have ongoing projects to merge network operating centers for different geographical and technical domains into "super-NOCs."

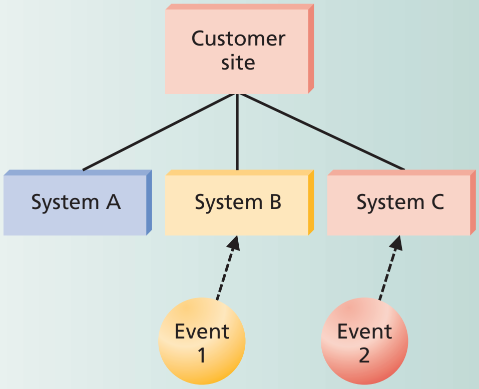
Another major effort toward greater efficiency is automating network management activities, such as automated alarm correlation, trouble ticketing, and alarm enrichment.

Interface management

Network management solutions are often huge software integration projects. A cost and complexity driver is managing interfaces, interface versions, interface documents, and so on. Current point-to-point integrations make the integrated network management solution sensitive to changes in interfaces and information. To make matters more difficult, telecom equipment vendors are not always keen to provide easily accessible management interfaces, which contrasts sharply to the norm for IP devices.

Contrary to rules and best practices, management interfaces often are not backward compatible. When equipment is upgraded, the previous integration work is often destroyed.

Figure 1. How a service model might map events.



Correlation software maps a low-severity event and a medium-severity event into the service tree and updates the service tree with the events' impact, making the overall severity for the service medium.

WAYS TO IMPROVE

Given these problems and changes in the environment that will affect network management in the future, we believe the next generation of network management solutions must be based on principles different from the current solutions.

Service-centric network management

At the core of a network management solution for the future lies a service model. Operators must have full control of the services provided to and used by customers. The service model must capture a service's semantics and its real-time status. Although service would be the model's primary focus, the model must still map other concepts such as resources, network topology, and customers. This model is far from trivial. It requires a strong formalism that can express relations and dependencies.

Figure 1 gives a flavor of how the model might work with a simple case. When two events arrive, correlation software maps them into the service tree and updates the service tree with the events' impact. In this case, one low-severity event and one medium-severity event arrive on different systems, making the overall severity for the service medium.

A modeling formalism for a service-centric view must be transformable. More specifically, it must be possible to pivot the "service graph" around the node of interest, so that the same model can be used to satisfy the district manager, the general manager, the technology domain manager, and the help desk manager at the same time. Current models with simple aggregations and so forth are far too primitive. Anyone who has used a service-management tool is familiar with the problem of services always being in a failed state because the models are too weak in expressing dependencies. This is not only a modeling problem; an even more challenging task is to maintain the model's actual instances. At all times, the model must be correct and mirror the network's actual state.

The most interesting attempt we have seen in modeling is the Distributed Management Task Force's Common Information Model (http://www.dmtf.org/standards/cim/). CIM has several good aspects. It has a service-centric model, emphasizes relationships, and maps resources and network topology to the service model. However, CIM has weak formalism—Unified Modeling Language static class diagrams. We do not see UML classes as strong enough in expressing such items as semantics and interfaces. Also, CIM's model complexity and size has exploded. Modeling every aspect as classes yields a huge model that will not cope with the changing and dynamic nature of the future services and networks.

Interfaces for network management must be much better defined, requiring appropriate standards for content and communication.

The IETF made an attempt to take SNMP one step forward with the SMIng data definition language, (*SMIng: Next Generation Structure of Management Information*, IETF RFC 3780, F. Strauss, TU Braunschweig, and J. Schoenwaelder, May 2004; ftp:// ftp.rfc-editor.org/in-notes/ rfc3780 .txt), which makes SNMP MIBs capable of holding objects, structured data types, and so on. SMIng has a pragmatic approach and would probably make a significant difference in the short term, although it has not created any footprints in the industry as yet. Attempts from the IETF's Network Management Research Group have the big advantage of being down to earth and well engineered. In the long run, however, something more powerful is needed.

From a solution point of view, service-centric network components are emerging—for instance, Cramer or Granite.

These product examples are signs that the field is moving in the right direction. Topology must be a core component, however, and the current solutions and tools do not handle the dynamic nature of the topology changes. Typical implementations use an export, clean, merge, and load process to create an overall topology database. To be fair, the fault is not with the topology tools themselves but with the poor equipment interfaces ("Managing Highly Dynamic Services Using Extended Temporal Network Information Models," R. State, O. Festor, and E. Nataf, *J. Network and Systems Management*, vol. 10, no. 2, June 2002, pp. 195-209).

Dynamic network management strategy

Network management mechanisms and solutions must become much more dynamic to cope with the changing environment, heterogeneous networks, dynamic services, and customers that come and go. In practical terms, dynamic network management has four main requirements:

Integrate network elements. Interfaces for performing network management must be much better defined. This will require appropriate standards for content and communication. We foresee an approach totally different from current technologies: Strongly typed interfaces, with patterns for interaction, will facilitate easier, but never automatic, integration among parts.

Optimize models. Topology and service models must be self-maintaining. This will require a fully integrated provisioning chain so that the models are always up to date. Also, network elements must publish dynamic interfaces for publishing the models.

Develop heterogeneous networks and dynamic services. Service requests, service discovery, and service capabilities must be handled in a dynamic real-time fashion ("Dynamic Service Management in Heterogeneous Networks," M. D'Arienzo, A. Pescapè, and G. Ventre, *J. Network and Systems Management*, vol. 12, no. 3, Sept. 2004, pp. 349-370).

Cope with change. Networks change more quickly every day. Systems must be dynamic and able to manage change.

Knowledge management

Operators we interviewed also stressed that they are too dependent on individuals and that their systems apply too little automation. Expert users with several years of network management experience are invaluable, but it's hard to reuse their knowledge because the processes are still carried out manually. The next generation of network management must apply knowledge management and expert-systems technology. This process will enable the solution to evolve, adapt, and capture the operator's knowledge and make the system self-learning and more automatic.

Such technology can capture network administrator usage patterns in real time and analyze them to produce a list of suggested automations ("Rule Discovery in Telecommunication Alarm Data," M. Klemettinen, H. Mannila, and H. Toivonen, *J. Network and Systems Management*, vol. 7, no. 4, 1999, pp. 395-423).

The key is to have a system that is self-learning and self-adapting, so that it captures the expert users' behavior and provides tailored responses. Thus, rather than implementing every scenario using traditional development techniques, network administrators are actually adapting the solution as they work.

Challenges and changes in the environment

In addition to the problems we identified in our interviews with operators, we see many external factors that affect network management. These include (IP-based) services such as VoIP, managed voice, and streaming media; new technologies like IP Multimedia Subsystem; increased requirements from customers regarding availability and quality; convergence of mobile and fixed networks; and ad hoc customers, services, and network access. Customers also expect roaming between operators and access to networks and network technologies to occur without disruption ("Port-based Multihomed Mobile IPv6 for Heterogeneous Networks," C. Åhlund and colleagues, to be published in *Proc. IEEE Conf. Local Computer Networks*, Nov. 2006).

We foresee a broker layer between users and network/service operators that will let users automatically receive the service that best fits their profile when they are mobile. Users will pay the broker, who will pay the operator. This business model will put even more emphasis on how service providers express service capabilities and features.

Equipment vendors have been experimenting with different protocol technologies rather than providing easy-to-use, high quality interfaces.

Network management interfaces

We also anticipate great progress in the design of network management interfaces. For a long time, equipment vendors have been experimenting with different protocol technologies rather than providing easy-to-use, high quality interfaces. Today's demand for ease of integration and automation will drive the industry to apply simple techniques like SNMP, but with a high degree of functionality and standards. We recommend the following best practices:

- Focus on functionality and quality rather than complex technologies.
- Provide an underlying model for topology and services.
- Ensure backward compatibility. An upgrade or change of software should not affect the interface.
- Find ways that will let operators integrate equipment more smoothly into their overall management solution.
- Use dynamic approaches in interface technologies. Minimize the need for external data.
- Filter and correlate alarms before sending them. Send problem-oriented alarm states pinpointing the affected service rather than low-level symptoms.

We also see a strong need for improvements in modeling formalisms to express service models and more dynamic semantic interface definitions. An even more important issue is the quality of the models themselves, irrespective of the modeling formalism.

In many ways, network management problems have changed little since 1988, when SNMP was introduced. There is still no sense of how to model management information and no greater insight into which information is truly valuable to a management application.

Progress requires investigating fundamental modeling questions: What characterizes a good model? Given a bunch of such models, what are the common structures, design patterns, ways of thinking, aggregation models, and so on? And given common denominators of good models, the problem becomes how to construct tools that let developers build such models easily. Is it even possible to develop a structured theory of network management that truly starts small and builds on real-world knowledge?

Telecom network management solutions need to shift perspectives from one of network element management to service management. Operators need a service view of their network, with automatic service-impact correlation. This requires some major changes in the underlying solutions: equipment vendors must improve the supplied management interfaces and network management solutions must implement a higher degree of automation and correlation with a service focus. One obstacle is the lack of models and formalisms to describe topology and service structures. We're currently working to define a formal service modeling approach to enable the service layer. ■

Stefan Wallin *is a network management solution architect and senior partner at Data Ductus and a researcher at the Centre for Distance-Spanning Technology at Luleå University of Technology. Contact him at stefan.wallin@dataductus.se.*

Viktor Leijon *is a graduate student at Luleå University of Technology. Contact him at viktor.leijon@csee.ltu.se.*

For further information on this or any other computing topic, visit our Digital Library at http://www.computer.org/publications/dlib.