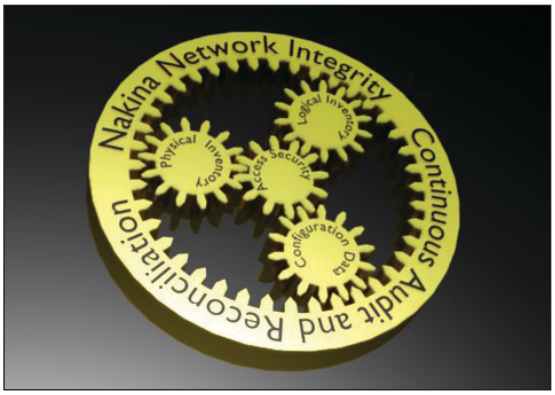
Pipeline
Your OSS/BSS Information Source.
www.pipelinepub.com Volume 8, Issue 3

Building a Network Integrity Practice

By Doug Bellinger, Nakina Systems



Industry best practices in telecommunications have, for many years, been tolerant of data integrity levels of 60 to 80 percent. As long as services operated in silos and operations staff could keep up with network growth, this was expensive and inefficient, but not mission critical. Nakina Systems has a unique perspective on why this can no longer be tolerated, and how a holistic approach to physical inventory, logical inventory, and network configuration can significantly improve data integrity levels. With this approach, it is possible to achieve data integrity in all of these areas, across all of the network elements and systems. This is how data integrity becomes Network Integrity.

Recent experiences with wireline, wireless, and cable operators have shown that two important things have changed:

- Everything is becoming IP connected, with all services sharing common IP infrastructure.
- The race to add capacity, especially to mobile data networks, is pushing traditional approaches beyond their breaking points.

Network configuration errors have always been, and continue to be, the primary source of service- affecting problems. Now, because everything is IP connected, every misconfiguration of the network creates potential exposure to fraudulent or malicious access. In addition, configuration errors can more easily affect multiple customers and services. Although “Next Generation“ OSS and BSS systems have automated the most repetitive and expensive tasks at the service provider, they have failed to deliver Network Integrity. The reasons for this include:

1. Each OSS or BSS has its own abstract view of the network.
2. Each system tends to “fire and forget“ its configuration changes, assuming that a successful configuration will be permanent.
3. Break-fix cycles, capacity expansion, network

upgrade, and performance management continue to require manual interaction that is error-prone.

Traditionally, Network Integrity has been treated as an expensive recurring project or simply a firefighting activity to patch problems. Audit and reconciliation projects would be undertaken when one of the following issues became intolerable:

- Asset utilization was unacceptable;
- Order fallout was at much too high a level;
- Outages became too large, frequent, or embarrassing to manage.

Any of these cases would trigger the service provider's "Immune System", resulting in an array of projects that would bring data integrity back up, perhaps to the 80% level that represents typical best practices. If these "Get Well" projects can be combined with "Stay Well" processes, operations staff can focus on future growth.

Business as usual could continue, except for one important problem: next generation services require 100% accuracy on a very large number of configurable parameters. To illustrate this, consider two important examples: security configuration, and service assurance.

In the first example, a single security misconfiguration can result in:

- An interface that allows inappropriate connections
- Equipment login for factory-default access being accessible to the internet
- Access to private information that can be exploited by hackers.

Recent examples on PlayStation network and with "News of the World" indicate the seriousness with which these threats must be treated.

For our second example of why the status quo is no longer adequate, consider next generation service assurance. In a typical carrier environment, a service creation environment and service activation system manage the design and configuration of a service, including provisioning the service and setting up

Traditionally, Network Integrity has been treated as an expensive recurring project or simply a firefighting activity to patch problems.

customer facing service assurance capabilities such as performance reporting and SLA enforcement. Provided the provisioning flows through without fallout, and all subsequent moves, adds, and changes are also automated, the configuration of a large number of components will have been orchestrated to deliver a sophisticated service with customer facing assurance capabilities. When fallout correction, break-fix cycles, or network upgrades require manual intervention however, all bets are off.

In both of these cases, anything less than 100% accuracy represents an unacceptable situation for the service provider. Only a holistic approach to network integrity, which combines analysis of network configuration data with the reconciliation of physical and logical inventory, can guarantee that services remain properly configured in the presence of these kinds of activity.

Bringing this kind of holistic approach to data integrity allows the same set of systems and processes to be applied to problems with physical inventory, logical inventory, and configuration management. The result is Network Integrity.

Physical inventory problems manifest themselves in poor asset utilization. Understanding which resources are available and which are in use allows service providers to manage acquisition of new resources and spare parts. Efficiency in this area results in lower maintenance costs, reduced inventory of spares, and higher return on capital. In one case, the savings resulting from aligning maintenance contracts with production resources was sufficient to pay for the entire lifecycle cost of the Network Integrity practice. The other benefits apply directly to the "bottom line".

In order to solve asset utilization challenges, the physical inventory in the network needs to be discovered, and compared to the inventory in planning systems. In many organizations, there are

a combination of systems with data for different network technologies, and administrative domains. This can be further complicated by environments that have been aggregated due to mergers and acquisitions. In some cases, the database of record may be file cards or spreadsheets. Since Sarbanes-Oxley compliance requires accurate reporting of assets, a great deal of time and money is often spent collecting and analyzing this information in recurring consulting projects. This money could more profitably be used to automate the discovery and reconciliation process, with the follow on benefits of being able to use the same data to support Network Integrity for logical inventory and configuration management.

Solving the physical inventory problem will improve asset utilization and support accounting for assets, but will do relatively little to improve order throughput or reduce outages. Reduced fallout (or improved throughput) requires an accurate representation of logical inventory, so that the resources designed for a service are used to implement it. Reduced outages require perfect configuration of these resources, as configuration errors account for more that 70% of network outages.

We've seen that automating these three classes of data integrity problem share a common set of solution requirements, and that these requirements are largely independent of the underlying network/service technology.

The reason that these solutions can be network technology independent is that the complexity is largely in three technology independent areas:

1. **Collect:** Collection of large amounts of network data in a secure and non- disruptive way. Data collection can't unduly burden the network, nor can it expose the configuration data to security risks. This class of problems must be solved once, enterprise wide, or the "silo" solutions represent another layer of exposure.

2. **Analyze:** Analysis of configuration data. The rules required to understand whether configuration data is within bounds are complex, but not dependent on the underlying data.

3. **Resolve:** Best practices for discrepancy resolution. The escalation, confirmation and correction processes tend to be enterprise specific, and technology, agnostic. Engineering these once, and applying them everywhere, is much more effective than allowing technology specific silos to behave, The implication of this is that a common set of practices and systems can be applied enterprise wide. This holistic approach can be achieved if a number of key challenges are met.

Reduced outages require perfect configuration of these resources, as configuration errors account for more that 70% of network outages.

The first challenge is secure access to network data. This may sound trivial, because every network element provides some combination of interfaces through which inventory and configuration data can be gathered. The challenge arises because the network integrity solution requires access to all of the configuration data. The combination of Command Line Interfaces, SNMP, web services API's, and legacy interfaces such as TL-1 require the data collection environment to support every kind of encryption and authentication available. Furthermore, the data collection architecture needs to be flexible enough to provide additional security when data is aggregated to a central site.

The next challenge is to provide flexible normalization and comparison logic. Each system that a service provider uses has its own data model, which is an abstract version of what is supposed to be in the network. Inventory systems contain a resource model that is used to design new services. Fault management systems contain a model that is used for root cause analysis and problem resolution. Performance management and assurance systems contain models regarding the utilization of the network. Each of these databases is an abstraction of the network data, and each needs to be accurate. By extracting raw configuration data from the network and applying flexible normalization techniques, a

centralized solution is able to ensure that these models are all synchronized with the network, and with each other. Traditionally, these problems have been addressed with separate projects per system. Not only has this traditional approach been expensive, it has also failed to provide a level of network integrity that would allow performance, fault, assurance, and inventory systems to all contribute to effective customer reporting and management strategies.

The third challenge is scale. If Network Integrity is to be maintained at a high level, then the service provider has to achieve a high level of scalability in three important areas: scalable data collection, rapid analysis and reconciliation, and scalable resolution.

Scalable data collection requires the data for the entire network to be collected regularly. Traditional approaches have tolerated this as a background task with baselines being collected on some interval. This might work well for asset utilization or flow through improvements, but will not address security threats or service assurance concerns. In order to achieve configuration data integrity, one more thing is required: data from individual elements needs to be collected and analyzed very quickly. To put this another way, the Network Integrity solution has to be optimized for both size and speed.

Speed is important because configuration processes are running concurrently.

A poorly assigned resource during a manual break-fix cycle may cause a fallout case that results in further manual rework. To avoid cascading errors, Network Integrity checks should be performed every time a manual interaction occurs with the network. In order to be practical, the results of this check should be available before the operator has moved on to his next assignment, hence the need for speed in analyzing individual elements.

Even if no manual interaction were taking place, the data and algorithms in BSS and OSS systems would sometimes collide with one another. This drives the need to check the entire network much more often than traditional audits would. A nightly audit of configuration data has a profound effect on Network Integrity levels, but requires a very scalable and secure data collection framework.

The Network Integrity solution has to be optimized for both size and speed. Setting up an NI practice has an immediate ROI through improved asset utilization

The final piece that's required to achieve Network Integrity is Gold Standard auditing. Each service provider conducts extensive analysis on how best to configure their networks to optimize service delivery. This knowledge is captured in methods of procedure, and in automation scripts and processes, and the configuration of provisioning and fulfillment systems.

Even so, things fall through the cracks. In addition to comparing the raw data from the network to the normalized data in OSS systems, the service provider needs to be able to apply rules-based analysis to configuration data. With such a capability in place, when a misconfiguration is detected, it will be easy to find. When a rule is changed, it will be easy to analyze the network for violations. The management of a Gold Standard dataset is essential to getting network integrity levels close to 100%. It is also essential to controlling operational costs as the amount of configuration data in the network continues to grow exponentially.

With the advent of cloud services and the mobile internet, capacity in the network is being added and changed at unprecedented rates, and services are changing the utilization of the network in real time. This environment will no longer tolerate periodic "Get Well" programs.

A Network Integrity practice can be set up that puts the service provider on an actively managed "Stay Well"program. There are significant technical challenges to succeeding with this practice, but these challenges are independent of the underlying network technology and can be deployed enterprise wide. Meeting these challenges has an immediate return on investment through improved asset utilization, improved network and service provisioning performance, reduced fallout, and the avoidance of costly outages and break-fix work.

About Nakina Systems:

Nakina Systems provides Network Integrity Management solutions to the telecommunications industry worldwide. Our solutions enable service providers to introduce new services and grow networks more rapidly and with fewer outages by automating the discovery of network equipment, reconciling with inventory systems, auditing software in the network, and centralizing management of network security. Nakina's solutions power integrity in the world's largest networks, and they are provided in partnership with the world's largest and most advanced equipment manufacturers.

Nakina's solutions work in next generation networks – whether LTE, Ethernet, IMS, or optical – where network complexity has increased. Our Tier I credentials have been earned by deploying solutions that achieve extreme limits of scalability, resiliency, and adaptability to changing requirements.

To learn more about Nakina Systems visit us at: http://www.nakinasystems.com/?src=pipeline_august