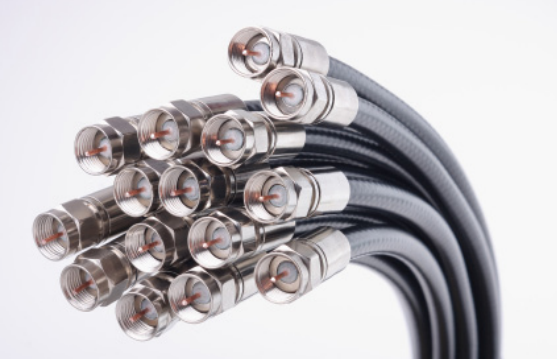
Pipeline
Your OSS/BSS Information Source.
www.pipelinepub.com Volume 6, Issue 11

Meeting the OSS Needs of MSOs

By *Sergio Pellizzari*, Nakina Systems

MSOs have used their backhaul technology to collect and target SMB and Cell Tower backhaul applications.



In their quest for market share, telcos and MSOs have become serious competitors as each has crossed over their traditional market lines, leaving both to focus on triple play, quadruple play, Ethernet services to businesses, IPTV, video on demand and the digital home. Telcos have targeted residential services with fiber to the home initiatives like Verizon's FiOS and AT&T U-Verse. The MSO companies realized that they needed to look beyond their traditional consumer video for expansion, since there are signs that this market has maxed out in terms of subscriber growth.

In response, MSOs have used their backhaul technology to collect and target small and medium businesses and Cell Tower backhaul applications. This means that most MSOs continue to maintain an RF-centric access to the home network, as well as a backhaul network that is becoming more and more focused on delivering Ethernet services directly to businesses or, specifically, to provide cell tower backhaul services for wireless service providers.

There have been early signs of success from the MSOs, but one large factor remains: MSOs need not only a competitive offering, but an OSS infrastructure in order to provide the same level of service that a telco would provide for a similar offering. As operations for these services have become more complex, the OSS problem has grown exponentially. For the most part, OSS and business support systems have not consolidated to keep pace with the changes that have been made with technology across the industry.

Today's MSO networks have different OSS problems than the telcos face. They face a steep learning curve. Even though they have the technical competence to provide the service, they have to set up administration and support for some very demanding customers, which now include businesses and wireless companies that are seeking strict adherence to Service Level agreements. Furthermore, some OSS software has some key architectural challenges when it needs to operate in an MSO environment. Cable operators have found that they need to step up to plate and include a solution that provides network integrity in order to satisfy the network guarantees that are required.

Some OSS software that interacts with Network Elements has been designed such that agents must be embedded with the equipment in order to perform monitoring. This design is puzzling. These agents need to be certified by equipment vendors since they are not embedded within the Operating System and are highly dependent on the software running on the Network Element. Equipment vendors are very reluctant, if not vehemently opposed, to externally developed software running on their network elements unless they are 100% confident that this software will not negatively impact the performance of the element. Certification adds more work and yet more dependency which simply adds more risk to an equipment vendor.

MSO networks also tend to be highly regionalized, which poses challenges for OSS software that

needs to interact with the network. Architecturally, this causes significant challenges for some OSS software which has been designed assuming ubiquitous access to network devices and not expecting firewalls between regions. A multi-tiered OSS software architecture works very well in these regionalized networks since a tier is specifically designed to be placed in the regions and other components in a centralized location. With this design, very specific ports between servers for the OSS solution can be opened minimizing the risk to the OSS network.

The only options for OSS software that interacts directly with the network require an architecture of independently deployable agents that can interact and collect information from a wide variety of network devices simultaneously and can be independently deployed in the regions and not embedded on the network elements themselves.

Another difference stems from the fact that the traditional MSO HFC or access network contains many network elements that do not interact extensively with OSS systems, since many elements are passive resulting in a very large dependency on GIS systems to track and capture physical network attributes. Any reconciliation against that system is strictly manual.

OSS solutions need to be just as agile to keep pace with a constantly changing network.

The new Fiber-oriented, Ethernet backhaul networks are far more active, and now capable of having OSS systems monitor network status, performance, and obtain network topology as well as the physical and logical inventory of the network. The discovery of the physical and logical inventory as well as the topology and reconciliation of live discovered data from the network against a planning inventory system is a new concept to MSOs simply because older HFC and access network simply did not have discovery capabilities.

MSOs have always had actively changing networks(much more so than telcos) and this most likely stems from a consumer oriented network where changes to the HFC plant for traditional cable subscribers or CMTS changes for Cable Modem subscribers are constantly changing. This flexibility and agility has translated into commercial Ethernet and Cell Tower backhaul applications. As a result, OSS solutions need to be just as agile to keep pace with a constantly changing network. Some OSS solutions in the Discovery area are simply not designed to keep up with the network changes. They have been designed for a much less active network where new markets are not quickly added or deleted, where customers are not changing their services very often, and where it might be acceptable to synchronize the network through discovery every few days.

With network elements being more active, the need for centralized secure access to network elements by operations staff is crucial. A multivendor, single sign-on system that can monitor and record all access to the network and provide a centralized methodology for security personnel to control

and audit this new network gear provides a key operational advantage. In addition, this security function will alleviate the chore of the operations staff to remember the plethora of independent vendor specific passwords or shared passwords that might be configured without such a single sign-on system in place.

It will become important with the deployment of large numbers of small devices (like Ethernet NIDs) that OSS solutions can audit network parameters and highlight discrepancies from "Gold Standard" settings which ensure network integrity. Without a network integrity solution, operations staff would be expected to manually log into every network element and "stare and compare" individual parameter settings on each and every device which is obviously time-consuming, tedious and error-prone (and completely unmanageable in a network of size!).

As MSO networks begin to focus on Cell Tower backhaul and commercial Ethernet applications, it is crucial for MSOs to also focus on their OSS infrastructure. It is just as critical for OSS solution providers to ensure that their solutions are architected in such a way that they can operate efficiently and effectively in the unique MSO environment.

The need for centralized secure access to network elements by operations staff is crucial.

To quote a good friend of mine in the MSO space, "Your competitor just looked at me like I had three heads when I told them of some of the specifics requirements to work effectively in our network." To which my response was, "Well, they really aren't our competitor, then, are they?"

About Nakina

Nakina Systems, the network integrity company, enables service providers to avoid outages and efficiently manage rapid growth of new distributed network infrastructure such as LTE, IMS, FTTH, and cloud applications. The company's solution portfolio is based on the ultra-scalable Nakina Network OS operations platform, and includes Intelligence applications such as the Network Integrity Controller, an automated network software audit and gold standard discrepancy manager, and the Network Discovery and Reconciliation Manager, an online network inventory discovery solution and Network Security and Single Sign on, a comprehensive credential system with secure access and video logging capabilities. Nakina solutions are used by three of North America's top five service providers, and delivered as OEM products by three of the world's top ten communications equipment providers. The Nakina Network Integrity Controller allows authorized users to perform manual and scheduled audits to determine the configuration settings on network elements

(NEs) that are being managed. Audits compare the configuration settings on one or more NEs to a baseline dataset which describe the expected values in terms of "Gold Standard" values and rules. Audit results show the discrepancies in snapshots that can be viewed, compared to other snapshots, or compared to live NE configurations. Scheduled audit results are automatically emailed to one or more recipients for analysis. Network Integrity Controller uses the user security features of Nakina to provide profile based protection of access to network information. Each Network Integrity Controller user is assigned their own set of unique credentials. Through role based access control, system administrators can define which network elements a user can access and control the functions that a user is allowed to perform. All user actions are logged and stored in the Nakina database. Audit data can be exported to reports that can be saved in a number of useful formats and imported into spreadsheets.