Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 6

Looking Past the Shift

by Duby Yoely

There are a few fundamental changes taking place in both network architecture and in the business landscape with which OSS deployments must keep up if telecom operators are to succeed in this extraordinarily dynamic market.

The increase in IP and next-gen networks have created conditions in which each player must deal with a greater number of partners and competitors. Traditional roles of many market players are changing as providers leverage the new technologies to offer new services and break out of their traditional "silos." Along with various incumbents entering each other's markets, the increased flexibility presented by network technology has enabled a rapid increase in the number of VNOs and MVNOs in many areas.

In addition to these market developments and stricter QoS requirements, the technological shift toward IP or next-gen networks itself brings challenges for network operations. Of course, it is difficult to discuss the challenges from technological developments and the challenges from market developments as separate issues, as each takes place in the context of the other. Ironically, the same technology that enables such commercial innovations as VNOs and MVNOs, also raises the risks for the smooth and profitable operation of their services. IP and next-generation Mobile technologies force operators – both VNO and incumbent – to face new operational challenges. Meeting those challenges may mean the difference between success and failure of the whole model.

Each class of these new market players introduces a unique set of challenges for network operations and OSS. Regarding providers of IP-based services (namely, VoIP providers), the key challenge is to guarantee QoS at a level comparable to that of circuit- switched networks. When VoIP was in its earlier stages, it was more of a novelty than a serious business proposal. QoS was not much of an issue, since the fact that it worked at all was impressive enough. This still applies to many cases today, especially with internet calling services such as Skype (although even there, one can see constant improvement). QoS is still not committed, but being a practically free service, they can get away with it. At the same time, these services fill a rather small market niche, with limited growth prospects at the current level of service reliability.

More serious VoIP providers wish to grow beyond a market niche and make this technology a mainstream means of voice communications and eventually reach a new universal standard. However, if these providers are going to grow their market share while keeping prices at a profitable level in order to successfully compete with the circuit-switched world, it is absolutely necessary that they also raise QoS to the same level. Similarly, current TDM incumbents who wish to migrate their voice services to IP and benefit from the efficiencies of packet-switched traffic will have to do so without compromising on quality. Regardless of how much these providers may invest in their network switching and transport hardware, they will be able to meet the tight QoS requirements of this business model only with a robust service assurance solution in their OSS platform.

One reason QoS is such a critical issue in VoIP is the same reason that applies to IPTV, mobile video, and similar content services: unlike data, user experience for voice is far more sensitive to traffic irregularities or packet loss. In addition to the QoS of the service while in use, VoIP also must address network availability in a stricter way than video services. If a network providing video services has some down time, this will create a very irritating experience for the user, with a very low threshold before leading to subscriber churn. However, as aggravating as video downtime may be, loss of dial tone is something that most subscribers don't even want to think about. Even to the extent that VoIP is already being adopted for its greater efficiency, there are subscribers who still maintain a PSTN line as well, just to be safe. If VoIP is to be seen as equally dependable, one bad episode of downtime and the resulting anecdotes of people unable to dial 911 can cause long term setbacks for the individual operator and VoIP as a whole.

If VoIP services are to compete with PSTN (or IPTV with cable), they'll have to continually monitor services in a way that fault resolution will be as proactive and near real time as possible. Consequently, they will need access to an end-to-end view of their network, their customers and services. The fault detection and resolution cycle must be automated to the greatest extent possible. Sophisticated analysis and reporting tools will also have to be part of such a solution, in order to allow operators to prioritize resources and maintain control over the various automated and manual processes.

The first step in this direction is a unified mediation layer, based on which many of these other capabilities are made possible. Once this layer is in place, the OSS tools can evaluate network events and other data in the context of the entire network topology, enabling intelligent automation of root-cause analysis. With an end-to-end network view and unified mediation layer, the most likely cause can be identified even if the corresponding alarm has yet to be received.

This level of automation can have a major impact on fault resolution speed, bringing root-cause identification to near real time, but it is still essentially a reactive process. It is now possible to actually move forward and proactively predict service degradation in many cases and prevent it before it actually occurs, largely due to the fact that most degradation these days is related more to traffic congestion than faulty hardware. This proactive capability can be achieved by the integration of a rich variety of data resources through the unified mediation, including both fault and performance data. This includes sources such as CDRs, probes, and data from network elements. With this data, traffic patterns and other customer-generated KPIs and KQIs can be analyzed, and thresholds created based on historical information which can alert operators before the subscriber notices anything.

Looking forward, the next step will be to automate the corrective action process up to the single session level. However, this is expected to become viable for implementation only a few years from now, due to technological and psychological drawbacks.

Beyond the physical changes in network infrastructure, another important trend is that with the proliferation of VNOs, there is an increasing number of service providers who do not own their own infrastructure. Since VNOs generally do not have access to much of the network data, they'll be required to closely monitor customers and services at their end of the network. They'll rely on data such as CDRs, active probes, and basically many of the features that have been added to OSS beyond the original network management systems to create the end-to-end solutions mentioned above.

Additionally, they'll need to monitor traffic at the other end, between themselves and their infrastructure provider, to ensure that inter-partner SLAs are kept. In fact, this aspect of QoS monitoring will soon have to encompass more than just a VNO and its infrastructure provider. The business environment is already shifting towards a multidimensional landscape, with several layers of providers (infrastructure, services, VNOs, and other third parties), and VNOs are aware that they often share their infrastructure provider with other VNOs as well. The many SLAs set throughout this environment target various QoS levels and often can be defined in different terms. In order to manage their rights and obligations as virtual entities with limited access to network data, the key here will be an emphasis on solutions with robust and flexible data manipulation. The OSS will have to allow the operator to define their own KPIs and KQIs to match each SLA, and to obtain the maximum amount of information that can be derived from the available data resources. In the future, there will likely be additional data sources created for VNOs as this trend continues and demand increases.

At the same time, the incumbents who own the infrastructure have their own

challenges. They'll need to be able track each user's traffic across the entire network, including both their own subscribers as well as those of multiple VNOs, in order to prioritize traffic and manage their multiple obligations. Following any network event, these providers must not only locate the fault within the network, but also be able to view it in terms of the users or services to be affected. There are already service-impact analysis tools which provide this capability. In fact, such solutions are already deployed among providers who service high-value business customers or sensitive services which need to be prioritized; when supporting multiple VNOs, this approach is all the more critical for a rational prioritization of network resources.

New network architectures and ownership structures are creating functional challenges in assuring QoS, and yet the end result must be on the highest level ever, due to increased competition. Only with advanced service assurance OSS will operators obtain the capabilities to manage their position regarding partners and competitors, and keep their key customers happy. In this shifting and dynamic market, with various PSTN incumbents, cable operators, IP providers and VNOs entering each other's markets, a reputation for high service quality will be one of the main benchmarks to indicate which providers will survive the current shift and come out on top.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.