VENDEOR PROFILE

A Network Services Response to Exploding Telecommunications Complexity

Sponsored by: Cisco

Andy Hicks

IDC OPINION

- The networks and IT environments that support telecommunications services will continue to grow more complex. Many communications service providers (SPs) today have embraced an architectural vision of converged networks, and are racing to roll out a rich set of revenue-generating services. These SPs face increasingly acute technology management challenges as they grow their service portfolios.

- At the same time, SPs must increase their speed to market for new services without disrupting existing services or the performance of their enabling environments.

- Assurance – whether service assurance or network assurance – is therefore a critical area for many SPs. Assurance addresses customers’ increasingly critical reliance on network and network-based services and is a key aspect of customer experience management.

- Cisco has substantially expanded its assurance offerings, which range from basic product-attached technical support to full operation of a given system. The guiding principles of Cisco’s portfolio are flexibility for the SP, a global service infrastructure, and automation of the intellectual capital that Cisco has gained from its central position in IP networks.
SITUATION OVERVIEW

Technological and Business Complexity in the Network

To say that the telecommunications industry keeps reaching new heights of complexity is stating the obvious, but that does not make it any less true. SPs are seeing wide competition for new business models while margins fall on their core services. They thus face the dual challenges of cutting costs while developing, deploying, and supporting new offerings.

Many departments have a stake in these efforts, but the network remains the enabling platform. The CTO's office must support growing numbers of new services and the new architectures that enable them. At the same time, the common IP infrastructure that underlies them all can make it harder to diagnose a fault, and makes it more likely that a bottleneck in one part of the system can affect multiple services. Since each service partakes of common resources, heading off impending performance problems is a consistently critical part of telecommunications management.

For SPs of all types, technological progress presents a variety of new challenges: LTE extends IP to the RAN while requiring mobile SPs to grapple anew with providing voice services. Small cells and carrier WiFi integrate with the macro cell network, making network management more complex. Exploding usage places capacity strains on all networks, at the same time as quality-of-service requirements are increasing.

As if pure network complexity were not enough, SPs experience additional challenges every time they add a new architecture for value-added services. These services are generally higher-margin, innovative offerings: unified communications and collaboration as well as various cloud models (infrastructure, software, communications, and desktop as a service, among others). In some emerging markets, basic consumer Web functions can be added to the list since they have not been definitively captured by over-the-top (OTT) players and can still be profitable for SPs. All of these services add new challenges in integration and management in areas where the SP has less experience.

From the business perspective, time to market is critical, most notably when it means that a SP can be first with a new offering. Every week that an SP can provide a service without competing offers from rival SPs or OTT players represents higher income and thus a quicker return on investment. Moreover, time to market is also critical in areas such as tariffing and marketing campaigns; in all three areas, faster development cycles generally lead to lower resources at risk and to greater success through more iterative development.

SPs are also dealing with the shift from a network-centric model to a broader one built around the information and communication technology (ICT) business. IDC believes that the integration of IT and network functions is one of the macro shifts the industry will experience over the next decade. Even today, IT systems are growing in importance inside SPs, both to manage functions like billing and customer relationship management and to provide multitenant enterprise services through a cloud or managed services model.
This expanded ICT portfolio presents integration and management challenges. In the long term, SPs will be able to unify the management of their network and IT environments; currently, however, they are managed separately. To succeed in each area, SPs will need to integrate data and control from across their technical environment, providing services and identifying potential trouble spots in real time.

**Customer Experience Management and Network Assurance**

One of the most common buzz terms in telecommunications right now is customer experience management (CEM). Like “cloud,” CEM is such an overarching term that it can apply to almost any vendor's offering; in some cases, it is used as a new label on an existing capability. Because it is such a broad concept, IDC approaches CEM more as a system-wide goal than as something that can be captured by a single, specific offering – a set of principles and goals that should guide the SP's long-term technical evolution.

At its simplest and most sweeping, CEM should involve collecting data from every part of the SP's environment, analyzing it in real time for usage patterns and service problems and providing that same view to any part of the organization that can affect the user experience, from network operations to customer support to marketing. The holy grail of this approach is per-user, per-service management in real time, although in practice SPs today still perform a fair amount of after-the-fact analysis and often model the experience of hypothetical user types rather than their actual customers.

One of the central pillars of CEM is assurance; making sure that users get the services they are supposed to and that all the enabling platforms operate within spec. The first consideration essentially corresponds to service assurance and is generally managed more in the IT environment, while the latter generally corresponds to network assurance.

While different vendors approach the problem in different ways, most are trying to move beyond a break/fix approach to a proactive/preemptive model. The goal of the industry is to diagnose and address problems before they significantly affect the user experience. This shift requires a high level of sophistication in at least two areas: integration, so that the assurance system can communicate with all the technical components and services that are running; and analytics, so that the assurance system can comprehensively monitor technical functionality, alerting administrators to both degraded performance indicators that could harm service quality and those that could lead to outright failure.

**Assurance, Financial Management, and Technical Evolution**

Finally and inescapably, there are financial concerns. SPs must add capabilities at the same time as they cut costs. This double bind often leads SPs to either outsource their network and IT operations to third parties or to retain internal control of their networks but reduce costs by offshoring some of their operations and support personnel.

Another related strategy is network sharing. Whether passive or active, sharing reduces an SP's ability to compete on network quality and coverage. The quality of services and the performance of the core network thus become even more important.
Corporate-level activity increases complexity as well: mergers and acquisitions bring together disparate networks and stores of service data that can require years of integration. Even all-IP networks take time to merge. And if a carrier group wants to introduce efficiencies among its affiliates by sharing functions across national boundaries, assurance takes on another level of complexity entirely.

Once the technical and portfolio strategy is set, financial engineering comes into play. CFOs must balance CAPEX against OPEX spending. With their CIO and CTO colleagues, they must decide which functions will be managed in house and which they will outsource. Especially in less developed markets, this group must also set the balance between reliability targets and the expenses required to achieve them, as well as charting a strategy between constant improvement and extending the life of their assets. No matter the direction a vendor chooses, financing and cost will be critical factors.

Even if an SP gets its service strategy completely right, it is still hard to manage and maintain the environment that enables it. Complexity is inevitable; the trick is to reduce the impact that complexity has on operations.

The key, therefore, is to manage the risk of service development. The technology/portfolio strategy must keep the time-to-market cycle short, not only to beat the competition, but also to test what works and what does not. Like many other aspects of telecommunications, service strategy has traditionally been slow, centrally planned, and conservative. To compete successfully, any business – and especially SPs – must enable frequent, iterative, and diverse service releases, gauging the market’s response to its services by releasing more and more of them. Enabling that strategy places increasing demands on both the technical architecture and all of the SP’s partners.

Cisco’s Assurance Framework

Cisco has long believed that an intelligent network is central to telecommunications success. The network’s centrality is both a blessing and a curse: On the positive side, SPs have deep expertise in their networks; on the negative, they may not have the skills or resources in house to support the exploding demands placed on them. Moreover, SPs need to keep pace with competition, requiring a service velocity that places burdens on change management. As an SP introduces more and more services, intensified demands on shared resources increase the risk that a new function will break existing capabilities. A similar “curse of success” inheres in capacity management: The more usage a network sees, the more likely it is to experience bottlenecks. Cisco’s service offerings are designed to support service quality by keeping the network healthy and preempting problems before they affect network performance.

Cisco places strong emphasis on its intellectual property as a competitive differentiator. Having deployed equipment in virtually all of the world’s networks, the company has amassed a wealth of experience and data on network operations and has invested in automating that knowledge in its service offerings. Given its dominance of the core routing market, Cisco believes that it leads the industry in operational expertise concerning IP core and fixed broadband networks, and that it has accumulated more knowledge about network operations than any single SP can boast. The company has also invested in its expertise in additional architectures, including hosted collaboration services (HCS) and cloud delivery models. Cisco will
provide a full range of services for several of these architectures in addition to the core network, often under a build-operate-transfer model.

There are four iterative levels of Cisco service offerings:

- **Base:** Like most solution vendors, Cisco has been offering a basic type of assurance service for years: Each piece of equipment comes with support and maintenance services that provide for things like troubleshooting, software updates, and replacement of faulty components. In Cisco parlance, this capability was formerly known as technical services and is currently known as base services. The company emphasizes, though, that it continues to incorporate new features into this base tier. For example, it believes that its network discovery and configuration management tools are among the most advanced in the industry.

**Figure 1**

One Services Portfolio (Subscription Services Packages Built on Increasing Capabilities)

- **Proactive:** Adding to the base set of reactive capabilities, Cisco is investing heavily in additional services that aim to forestall these problems. Under this structure, proactive services offer more active engagement with the system, including periodic network optimization exercises, as well as active management of software configuration, release management, and security patches. The guiding principle of this tier is that a system is less likely to fail if it is up to date, fully patched, and periodically audited.
**Preemptive:** Building on base and proactive is the preemptive tier, which moves assurance into the realm of real-time managed services. Preemptive services monitor myriad technical parameters in real time, generating alerts whenever those indicators exceed normal operations. These indicators include technical faults, but also operational data that Cisco's own analytics associate with degraded performance of the services that run on the network. Cisco’s experts then apply their knowledge of the customer's network to identify the underlying problem and recommend the optimal solution.

<table>
<thead>
<tr>
<th>TABLE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Preemptive Monitoring</strong></td>
</tr>
<tr>
<td>Focus Area</td>
</tr>
<tr>
<td>Objective</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Source: Cisco and IDC, 2013

**Operate:** Should the customer not wish to invest in all the resources necessary to address those alerts itself, it can engage Cisco at the operate level, where Cisco takes the data and capabilities contained in the first three phases and uses them to manage a given technical architecture on the customer’s behalf. Cisco prefers to call this relationship "out-tasking" rather than "outsourcing," a distinction that emphasizes that the customer retains ownership and ultimate control of their infrastructure, while Cisco applies its expertise to upkeep and evolution of specific pieces where it can add the most value.

Cisco underlines the cumulative nature of its Assurance Services tier structure: Each tier builds on the complete set of capabilities in the tiers before it. So, for example, the preemptive tier will monitor network performance against the parameters set in the optimization activities of the proactive tier. Likewise, the operate tier will incorporate the configuration and release management standards of the prior tiers.

In addition to the continuous cycle by which it automates the network expertise generated by its product development and professional service teams, Cisco also emphasizes that it has built a global service delivery structure. That organization centers around two Proactive Network Operation Centers (PNOCs) that collect network data in real time and generate performance alerts as well as suggestions for improvements. As any managed services provider must, Cisco has also developed local support capabilities around the world, including spare parts management and local language support.
**Building a Complete Service Package**

Every network has its own needs, and Cisco emphasizes its flexibility in drawing features and capabilities from across its entire portfolio to create a service offering that meets the needs of a specific business case and technical environment. As an example, one part of the network could be served with features from the proactive tier, while another part would be subject to the full operate tier. An SP customer can thus deploy its internal resources based on its own priorities, and engage Cisco to handle lower-priority functions and/or parts of the network.

To address the CFO-level concerns discussed above, Cisco also makes a variety of funding and ownership models available via Cisco Capital. This vendor financing could potentially include more software and services elements than a comparable package from a bank.

**FUTURE OUTLOOK**

As SPs provide more services with ever more finely differentiated quality, IDC believes that most of these companies will seek outside help in running their networks and ICT environments. Assurance is essential to customer value, and those SPs that implement best practices will inevitably differentiate themselves from their competitors. Cisco brings many advantages to its network assurance offerings, including its deep expertise in the IP core, fixed broadband, and other architectures, as well as its financial resources, global reach, and partner ecosystem. With its four-tier assurance structure, Cisco has created a flexible and full-featured set of capabilities to address the increasing complexity and operational challenges that affect most global SPs.

**Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2013 IDC. Reproduction is forbidden unless authorized. All rights reserved.