ORACLE
COMMUNICATIONS

# Building Networks for Competitive Advantage

## The value of monitoring your signaling network

ORACLE WHITE PAPER | JUNE 2016

ORACLE

## Introduction

The value of keeping their telecommunications networks optimized and trouble free cannot be overemphasized to service providers. After all, their network is what runs their business. Not only does it provide day-to-day revenue generating services, traffic on the network can yield invaluable information that can be used strategically to grow the business. Therefore it is important for operators to ensure their networks run smoothly. All too often, though, keeping networks running efficiently requires large outlay of engineering resources and hefty operating expenses, sometimes leading to suboptimal implementations, and insufficient attention to its continuing growth and evolution.

This document explains how service providers can realize the benefits of a well-run network and yet keep their maintenance budget in control.

## The Problem and Possibilities with Today's Networks

Today's IP communications are complex. The complexity arises from a variety of reasons:

- Sheer number and a diverse group of processing elements

  IP real-time communications networks now contain a variety of signal processing entities including gateways, call control, SBCs, application servers, authentication servers, policy servers, routing proxies, etc. Their numbers keep increasing responding to ever increasing traffic demands. Their deployments tend to be distributed and call flows are not always uniform. Diverse customers with sometimes conflicting requirements need to be accommodated. The result, sometimes, is an overly complicated placement of network elements which is hard to monitor and manage.

- The need to support several access methods and technologies, for example, fixed and mobile lines, hosted services, SIP trunks, WebRTC access, etc.

  Service providers today want to build a "converged" network – that is – a single set of resources that can be put to multiple uses. While this does reduce their capital expenses, it does introduce additional complexity into the way these resources need to be configured and operated. Proper monitoring becomes even more important to ensure they function trouble-free and are able to deliver as expected.

- Elements from a multiplicity of vendors whose implementations may not interoperate with each other

  Using more than one vendor is sometimes a conscious decision that service providers make in order to reduce their dependence on a single equipment supplier, to use best-of-breed offers, and to reduce capital expenses. Although this is a sound strategy, it does add to the complexity in the network since each vendor's implementation is somewhat unique even though they may be based on the same set of standard interfaces and protocols. Moreover, each vendor also usually has their own monitoring and management framework which makes operating the network as a whole even more difficult.

- Elements required to support new and increasingly complicated set of services, e.g., for address resolution, number portability, etc.

  Introduction of the new does not always mean removal of the old. Sometimes it might take years before older equipment can be taken out and replaced with new. During that transition time, special interfaces need to be put in place so that both can interwork. For example, number portability databases are generally located in legacy

databases accessed through SS7 based protocols. But IP systems still need to access and work with them in order to support that function.

» Continuing growth in traffic

Although growth in traffic is desirable and adds to operators' revenues, but as they add subscribers and evolve their networks to LTE with accompanying services such as Voice over LTE (VoLTE), Video over LTE (ViLTE), Voice over WiFi (VoWiFi), and Rich Communications Services (RCS), added traffic demands may outpace the ability of the network to handle it. If not carefully managed and designed for, it can lead to undesirable effects such as reduction in quality of service which may increase post dial delays, failed call attempts, have a negative impact on revenue, and contribute to customer churn.

In face of this complexity, operators struggle to keep their networks running at their full potential. But the stakes are high. While a well run network can be a strategic advantage for the operator, a network that has been put together hastily or over time without regard to appropriate controls can be a nightmare to operate.

On the other hand, an efficient network can accrue the following advantages for the operator:

» Maintain and enhance customer experience and reduce churn

It is clear that a well-designed and operated network can provide a competitive edge for the operator. Such a network would reduce customer complaints, ensure quality of service, reduce call setup times, and provide a consistent service level. Happy customers promote the service further increasing the revenue potential.

» Assure all SLAs are sustained

A network that has proper controls built into it can also assure that SLAs with other providers and with customers are measured and corrective actions taken in time before any parts of the agreement are breached. Such timely actions will satisfy customers and eliminate any unnecessary penalties.

» Anticipate and avoid traffic congestion

A network with appropriate measurements from its different elements will ensure that each is operating within its design limits and no individual link is being overloaded. If such situations are encountered frequently then the network should flag it so that the condition can be handled proactively.

» Advanced Analytics

With advances in data mining and emergence of analytical applications, there is a wealth of information that can be gleaned from traffic patterns and usage of the network, if only the relevant data can be collected and exported to such applications. This would help operators spot trends early, plan for them, and direct their marketing efforts appropriately. Such marketing may focus a marketing campaign to an appropriate set of existing and potential customers for increased uptake rates and reduced acquisition costs.

To tame the complexity of the network and to realize the benefits of a well-run network, operators need to monitor their networks closely. Clearly, such monitoring on a large network is not possible without monitoring tools designed explicitly to deal with today's complicated networks.

## Attributes of Good Monitoring Tools

Monitoring tools are essential to provide the deep insight required to turn communications networks into a competitive advantage. Some of the key attributes of a good monitoring tool are the following:

» Passive and non-obtrusive

A monitoring system should not interfere with the working of the network itself. Traffic should not have to be diverted specifically to flow through the system since that will add even more complexity and the possibility of errors. Ideally, the system should collect packets through built-in probes in some key network elements themselves. If it does have special probes, then these probes should simply collect data via port forwarding in switches without any configuration changes in processing elements.

» Vendor agnostic

Service providers frequently create their networks with components from different vendors. Usually each vendor's monitoring tool is usable only with their own components. Using such tools would mean fractured and partial views into the network which would not be optimal. Therefore, a tool that is designed to be vendor agnostic, work at the protocol level, and be able to smooth out differences in implementation is necessary.

» Service agnostic

Today's networks are called upon to deliver a diverse range of services. Access devices have different capabilities, access networks vary from fixed or mobile, customers range from enterprises to consumers, and services vary from basic audio calls to video conferencing and collaboration. The operator network needs to serve all of these variations in expectations. A good monitoring tool would be equally effective for the complete range of service offerings.

» End-to-end signaling capture and display

Signaling for a single transaction or session usually spans multiple network elements. For example, a call originating from a user device may be received by the network on an SBC which might forward it to a proxy for address resolution, which in turn might send it to a registrar function. The registrar may determine the destination and, acting as a B2BUA might send it to a GW for completion.

A good monitoring tool would be able to put all these signaling legs together as parts of a single session and display it as such to the user enabling them to view the call as it arrives in the network, the path it take, and as it exits.

» On-demand troubleshooting

Being able to troubleshoot and locate problems quickly in the network is of utmost importance to service providers. Studies have shown that this one attribute alone has a huge impact on customer satisfaction and goes a long way in reducing churn.

A good monitoring tool should be make it easy to determine errors by letting users drill down into message exchanges and review individual requests and responses.

» Intuitive and simple graphical user-interface

With the large amount of data a monitoring tool gathers and analyzes, the way that it displays that data to the user is crucial for the user to make sense of it. The data should be logically organized and allow the user to zero-in to the attributes they are interested in. For example, if the user is interested in finding out codecs being used in calls, the GUI should allow that. In addition, the GUI should be web based and be able to run without any special plug-ins, so that it can run as effectively on tablets as it runs on desktops.

» Multiprotocol inline display

Steps in call completion sometimes involve use of other protocols. For example, a call initiated with SIP may require a network element to use Diameter to check with a AAA server to ensure that the user is authorized to make such a call, or there might be an ENUM step required for address resolution.

In case of an error in call completion, a single ladder diagram display capturing and plotting all protocol exchanges would aid in rapid troubleshooting.

» Built-in and programmable KPIs

Key Performance Indicators (or KPIs) provide standards of measurement by which efficiency, performance, progress, or quality of the network is assessed. There can be hundreds of KPIs covering such measurements as number of active calls, number of registered users, call attempts made in the last hour, number of calls that failed to complete, post dial delay, etc. There are some standard KPIs defined by IETF but each operator is likely to have some derived metrics that is relevant to their own service and network.

A monitoring tool should provide a large built-in selection of standard and common KPIs and allow creation of new more relevant APIs customized to the needs of the operator.

» Media quality analysis

Delivering good quality media is crucial to service providers and so it is important for them to measure it and take corrective actions if necessary.

A monitoring tool should be able to measure and provide key information relevant to media quality such as number of lost packets, variance of delay between received packets (jitter), and delay in receiving transmitted packets. It should also be able to provide some commonly used metrics such as its MOS value.

» Secure and cloud enabled

Being able to deploy their applications in the cloud and find new revenue opportunities is becoming more common. Access to applications deployed in service providers' datacenters and offered as a service to customers, needs to be secured. Hence if a service provider offers monitoring as a service to its customers, the access to its dashboard as well as data from its probes must be encrypted through secure connections.

» Data export and reporting capabilities

Larger service providers usually create dashboards that provide summary views of different aspects of their business on a single screen. Underscoring the importance of the network in the business, a good monitoring tool should support APIs that allows these upper business level applications to pull relevant data from the tool.

In addition, a good tool should allow generation of management reports either natively or through export of data to a report generator.

» Scalability and aggregation

In these days of global carriers, monitoring tools should be able to scale up to their networks. While it may be difficult for any one system to keep up with a large geographically spread network, a good tool would be able to build a hierarchy that would aggregate results from individual installations to provide a global view.

» Virtualization

Following the lead ETSI has taken in defining NFV, most operators are embracing the technology and virtualizing their network functions. Although this technology is not ready for some network functions particularly those that handle and process media, a monitoring system should be able to be virtualized and supported on COTS platforms quite easily. This provides a lot of benefits to the service provider by being able to use standard datacenter hardware to host the application.

» Data Source for Analytics

Data and insights generated by the monitoring system are invaluable to the service provider. Even more so to departments outside the OSS group such as revenue management or marketing. Combining monitoring data with other data sources such as a subscriber database or customer feedback in a larger analytics application can act

as a key differentiator from other service providers. The revenue management team may decrease revenue leakage by detecting fraud and marketing can create marketing campaigns that are spot-on.

## Oracle Communications Operations Monitor

Oracle Communication Operations Monitor is a real-time, end-to-end service monitoring, troubleshooting, and analytics solution that provides unprecedented insight into Voice over Internet Protocol (VoIP) and unified communications (UC) networks. Oracle Communications Operations Monitor enables service providers to quickly and securely migrate to IP networks, reduce operational costs, increase subscriber and employee satisfaction, and minimize churn. Oracle Communications Operations Monitor also helps service providers with real-time troubleshooting of call quality issues with deep drill-down capabilities into both media and signaling—a true differentiator in the market. It is a proven, carrier-grade solution for fixed and mobile service providers with more than 100 deployments globally—including many tier 1 network service providers. Oracle Communications Operations Monitor is a data source to the Oracle Communications Analytics (OCA) family of analytics applications tailored to the communications market.

## Conclusion

The value of a properly monitored network cannot be overestimated. It really positions the operator's network as their strategic advantage over other providers. Oracle Communications products for network monitoring and data analytics can help operators increase efficiencies in their networks and realize the benefits. More information can be found on Oracle website:

Oracle Communications Operations Monitor:
http://www.oracle.com/us/products/applications/communications/operations-monitor/index.html

Oracle Communications Data Model:
http://www.oracle.com/us/products/applications/communications/industry-analytics/data-model/overview/index.html

Oracle Communications Customer Experience Analytics:

https://www.oracle.com/industries/communications/customer-experience-analytics/index.html

**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services



Building Networks for Competitive Advantage
June 2016