Zero Touch Service Assurance

A Technical Paper prepared for SCTE/ISBE by

Sean Yarborough
Sr. Director, Product Marketing
Lifecycle Service Assurance
Spirent
sean.yarborough@spirent.com

Table of Contents

List of Figures

List of Tables

Introduction: Metro Ethernet Service Trends

Today's telecommunications marketplace is experiencing a significant growth in the number of deployments and the types of services being deployed in the metro Ethernet or business Ethernet space. For example, small cells are a driving factor behind the need for increased Ethernet backhaul services. One of the reasons for this surge is the promise that small cells will deliver higher quality voice, video, and data services than ever before, with lower deployment costs than macro cells. Likewise, the transition on cloud hosted applications, VoIP networks, and the overall increase in bandwidth utilization are driving demand from enterprises for higher speed services. In order to truly reap the benefits of the small cell promise, cloud hosted applications, or any new technology, providers must ensure the quality of service demanded by today's end users and carriers. This paper explores key metro Ethernet service trends, the challenges these trends create for service providers and the benefits of transitioning to zero-touch service assurance to help address these challenges.

Metro Ethernet Market Trends

1. Ethernet port growth

IHS Technologies is forecasting worldwide 100G port revenue to grow at a 137% compound annual growth rate (CAGR) from 2014 to 2019. This growth is a must in order to deliver the volume of data and services required in the network of the future.

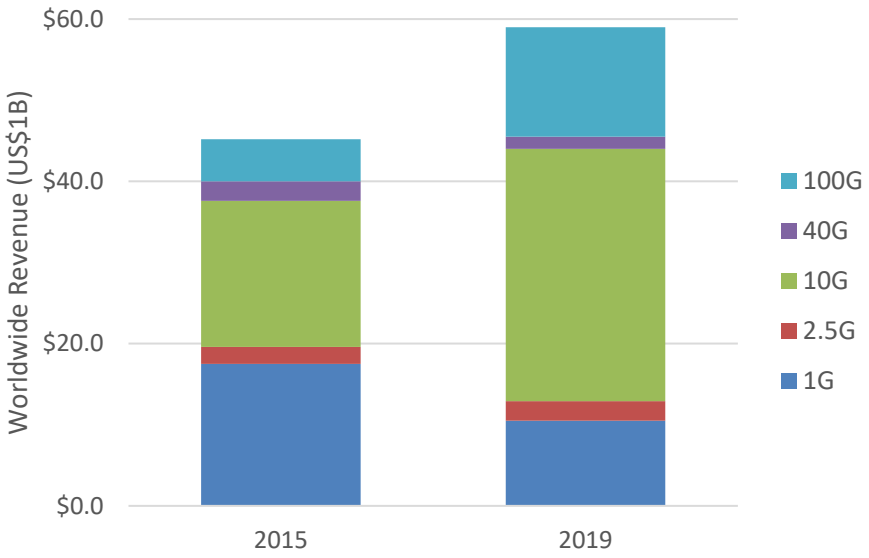

Figure 1 – 100G Port Revenue Expected to Reach $60B by 2019 (Source: IHS)

Another reason for the increased 100G surge is that the price per port has been declining over the past four years which is helping to driving demand. What used to cost tens of thousands of dollars, is now affordable to many providers, enabling them to offer cost-effective services above 10Gbps. And costs are only predicted to keep reducing, further increasing demand. As both the number of services being

deployed and the speed at which they are being deployed increase, providers must move to a holistic, automated, and intelligent approach to service assurance.

2. Stricter SLAs

According to a Global Service Provider Study by Infonetics entitled, Macrocell Backhaul Strategies and Vendor Leadership, "Latency is a very critical SLA metric, rated very important by 100% of respondents, followed by uptime/reliability, downstream bandwidth, jitter, and upstream bandwidth."

Data services are becoming more and more mission critical, while the speeds at which they operate are only getting faster and faster. And with applications being outsourced and hosted in the cloud, the need for continuous connectivity is no longer a luxury; for many it is essential. Today's consumers have clear expectations about the availability and the quality of their services and because of this, providers must track and be proactive about monitoring service level agreement (SLA) metrics.

3. Deployments of SDN/NFV Networks

Another issue that is driving increased usage and bandwidth consumption as well as an overall change in the market, is the migration to SDN and NFV. IHS interviewed current incumbent providers, competitive providers, independent/wireless providers, and cable operators who control 53% of the global telecom CAPEX and the universal position is that the industry is moving towards virtualization.

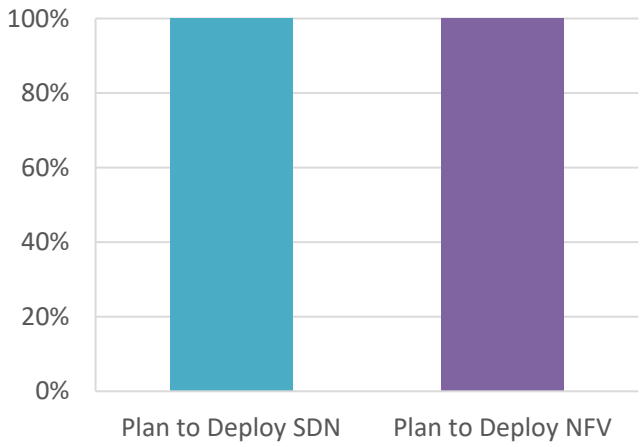

Figure 2 – 100% of Service Providers Surveyed by IHS Plan to Deploy SDN and NFV

No longer will applications run on dedicated, custom-built hardware. Instead they will be software-based micro-services running on a standard COTS "white box" platforms with compute resources. Virtualization will drastically change the way networks are deployed, managed, and maintained; therefore, a new level of service assurance will be needed to keep up with customer expectations in a virtual environment.

Service Provider Challenges

In this new paradigm, Service provider challenges to service activation and SLA management will fall into three categories. While these categories are not new, the way they must be addressed in this new environment is different. These challenges include:

1) Service Delivery
2) Trouble Management
3) SLA Management

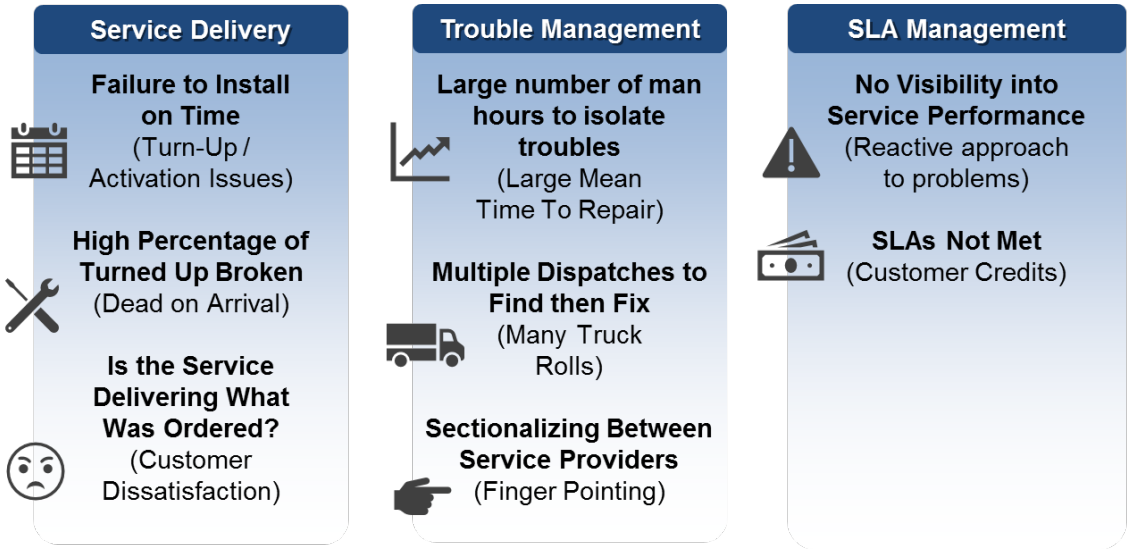

Figure 3 – Key Service Provider Challenges to Service Activation and SLA Management

1. Service Delivery Challenges

Service delivery challenges include failure to install on time (turn-up/activation issues), a high percentage of turned-up broken (dead on arrival) devices, and delivering the service that was ordered (preventing customer dissatisfaction).

Customers expect services to be turned-up very quickly (within hours or days, not weeks or months). This presents a challenge for traditional carriers who process orders by receiving a service order, putting that order into a queue, and scheduling a service technician dispatches to turn-up that service sometime in the next week. Today's customers want their services activated quickly and correctly the first time.

Another challenge with service delivery is trying to address the high percentage of services that are turned-up incorrectly or dead on arrival. As services become more complex, field technicians are not always equipped to install or troubleshoot services during their first customer visit. In other cases, the service may be "working", but not to the performance/SLA guaranteed to the customer, thereby initiating a trouble call. Often equipment is replaced unnecessarily which is costly and not always an effective solution.

Providers need to prove to customers that the services they ordered have been delivered. Gone are the days where a technician would install the connection and then run a PING test to verify installation. Today, providers need to be able to present a clear indication of how the service is being delivered, what level of quality is present, and assurance that the SLA is being met.

2. Trouble Management Challenges

Trouble management challenges include a large number of man hours to isolate troubles (large mean time to repair), multiple dispatches to find and then fix (many truck rolls), and sectionalizing between service providers (finger pointing).

Service providers spend a great deal of time trying to isolate troubles and this results in many wasted man hours. Even the simplest of problems can take hours of wasted manual intervention. The lack of automated processes and automated workflows only add to extended time to repair. And in some situations, SLAs are being violated just because of the lack of actual data from the network.

Some providers still subscribe the theory that “when in doubt, dispatch out.” This mentality creates a lot of truck rolls and often these truck rolls involve unnecessary equipment replacement, which isn’t a cost-effective way to manage these services.

When you have services that are delivered through an alternate vendor, type II services for example, the idea of being able to clearly sectionalize between providers can be quite a challenge. When services go to a third-party, the visibility into that service becomes severely limited. This is even more so when you are delivering metro Ethernet or business Ethernet services because the cable infrastructure, cable modems, etc. don’t necessarily possess the capability to provide the same level of testability, service assurance capability, troubleshooting capabilities that traditional service provider premise equipment (NIDs, network terminating equipment) have historically provided.

3. SLA Management Challenges

The challenges with SLA Management include poor visibility into service performance and not meeting SLAs.

The lack of visibility into service performance leads to a reactive approach to problems. This reactive mode is time consuming and unproductive and usually end up leading to an SLA violation or customers waiting longer than necessary for service restoration.

SLAs have liquidated damage clauses, penalties, etc., if violated. Having to pay fees for SLA violations drastically cuts into the profitability of the service.

Current Approaches to Service Activation & SLA Management

So how are service providers dealing with service activation and SLA management challenges today? For service activation, many providers are still dispatching multiple personnel who use handheld devices that can only test one circuit at a time and can be costly and don't scale well.

SLAs are often monitored with NIDs, which can certainly be a viable methodology, however each network interface device (NID) manufacturer has a different element management system (EMS) which work in slightly different ways, have different KPIs, and different capabilities. As a result, there are multiple systems that have to be simultaneously managed to truly have full coverage of the network. It's also very difficult to sectionalize when SLAs are not met using this approach because while NIDs can test end-to-end or point-to-point, they limited in their ability to segment the network and isolate faults. This makes troubleshooting problems difficult and ultimately leads to finger-pointing between the access vendor or type II provider and the provider.

Many providers use passive probes to manage SLAs. The problem with these tools is that they are very limited in terms of what type of data they can collect. Often, they are limited to the ingress UNI and do not provide an end-to-end view of the performance. Additionally, these probes only provide analysis when user traffic is available, so there is very limited visibility into issues such as loss, true availability, latency, jitter, and delay – issues that are extremely important to end-users. This solution also does not adequately support virtual and hybrid networks, which many providers are moving towards. The passive nature of these tools don't migrate well into a virtualized environment. The concept of "sniffing" a link in a virtual environment has some technical challenges.

Best Practices for Zero-Touch Automation

Spirent has compiled some recommendations for best practices which aim to achieve the goal of "zero-touch" service assurance for Ethernet and IP services. These best practices revolve around several key points:

1) Centralized, automated & intelligent Lifecycle Service Assurance
2) Use of global, industry-wide test standards (e.g., leverage CPE embedded features)
3) End-to-end visibility, troubleshooting & segmentation (e.g., "Dispatch to fix, not to find")
4) Integration of all dependent systems within a single Service Assurance Test Controller
5) Scalability to handle drastic service growth w/o large increases in OPEX

1. Centralized, Automated & Intelligent Lifecycle Service Assurance

The first best practice is the concept of centralized, automated and intelligent Lifecycle Service Assurance. This model purports that service assurance should encompass the entire network lifecycle from design, to onboarding, deployment, operations, maintenance, and back to design. Providers see the

need to provide a closed loop from design into operations and back to design to effectively manage network services as they migrate to the virtual space.

Figure 4 – Complete Lifecycle Service Assurance

There are 4 key functions that must be in place in order to implement a complete Lifecycle Service Assurance platform throughout the service lifecycle in the production network, which includes: active service activation, active performance monitoring, and on-demand troubleshooting (with passive monitoring and active testing).

Active service assurance enables consistent and repeatable activation tests, centralized storage of the service birth certificate, automated network element control, and multiple test methodologies that can be embedded into a service activation workflow.

Active performance monitoring provides the ability to really monitor the performance and availability of the network in real-time, 24x7, with comparison against SLAs on a service-by-service basis, and alarming and thresholding accordingly and the ability to push this data to external systems whether that is done by traditional methods by pushing reports on a regular basis or streaming that telemetry into a data link that can be accessed from northbound systems for analytics, policy mapping, etc.

Active performance monitoring allows for scalable, 24x7 real-time analysis of the network, monitoring and reporting, SLA and availability monitoring enables SLA management, native web GUI and NB interface to existing OSS.

Once active monitoring is in place, passive monitoring and active on-demand troubleshooting are used to isolate faults. Because of this integration, if an issue arises, the system can automatically execute a troubleshooting workflow, identify where the problem resides, and isolate that segment of the network before a tech is dispatched. If this can be done in an auto fashion, the time a tech is engaged is reduced from hours to minutes. This could be the difference between violating an SLA, having to pay liquidated damages, or not.

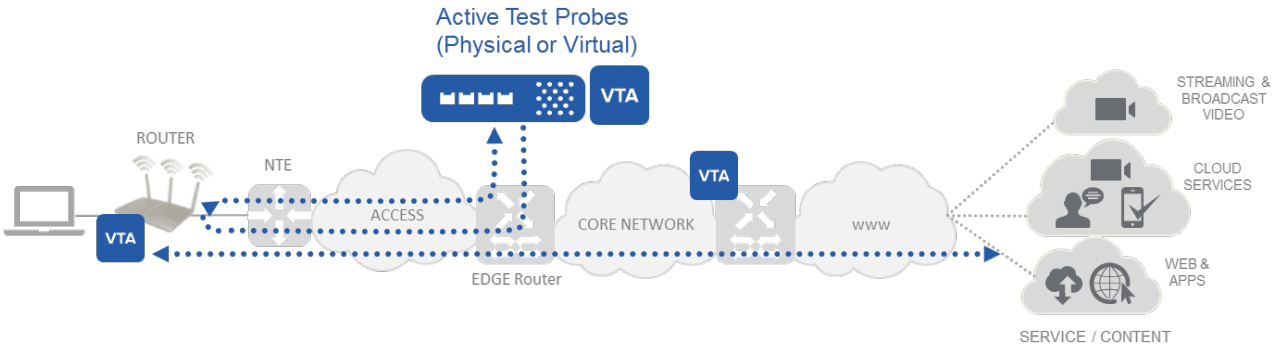

Figure 5 – Active test probes (physical or virtual test agents(VTAs)) for end-to-end service testing and testing of network segments.

2. Use of Global, Industry-wide Standards

The use of global, industry-wide test standards such as embedded CPE features and embedded network element features (e.g., MEF 46 latching loopback, Ethernet OAM, TWAMP, TR69, TR143, etc.) are crucial to creating a zero-touch service assurance platform.

In our global market, service providers, network owners and equipment vendors must work together to deliver telecommunication services to end users. Guiding them are the industry standards and requirements that help ensure services are reliable, cost effective and deployed properly in a timely manner.

The Metro Ethernet Forum (MEF) has developed a set of standards so that providers and vendors can work together in a harmonious way, using any vendors' equipment, and know that the same KPIs apply. Furthermore, this approach enables service providers to deploy service Assurance at the edge/core of their networks while leveraging already deployed CPE devices at the customer premises, providing a cost-effective solution for true end-to-end Service Assurance.

While some standards have been in use for years, like RCF 2544 for benchmarking and 802.1ag for testing loopback, delay and multicast loopback, there has been an evolution to more sophisticated testing to keep up the growing sophistication of the services and the supplication of the user's expectations.

Standards like Y. 1564 has been developed to replicate user traffic more realistically though a use of EMIX and burst testing and RC 6349 can perform TCP throughput testing. While these standards may have been developed for typical service activation, they also apply to service assurance for continuous network monitoring and guarantees that your service is delivering great quality, meeting customer expectations, and satisfying SLAs.

3. Automated End-to-end Troubleshooting & Fault Segmentation

By implementing a centralized test management system, providers can look through a single pane of glass to access all of their provisioning, trouble ticketing, analytics, reporting, and inventory systems. The test

manager is also automated and can automatically launch a set of standardized tests without human intervention.

True end-to-end visibility is also imperative to have a true view of the network. With access network and aggregation networks operated by local providers and the core network by a national provider, all using multi-vendor interfaces such as Accedian, Ciena, Cisco, ALU, Juniper, Arista, Rad, etc., there needs to be a seamless way to communicate with the variety of embedded test function in NIDs and other network elements.

By having true end-to-end visibility into troubleshooting and segmentation, faults can be isolated before a trouble ticket is generated. This allows any dispatch to have the goal “to fix, not to find” and creates faster time to resolution and ultimately higher customer satisfaction.

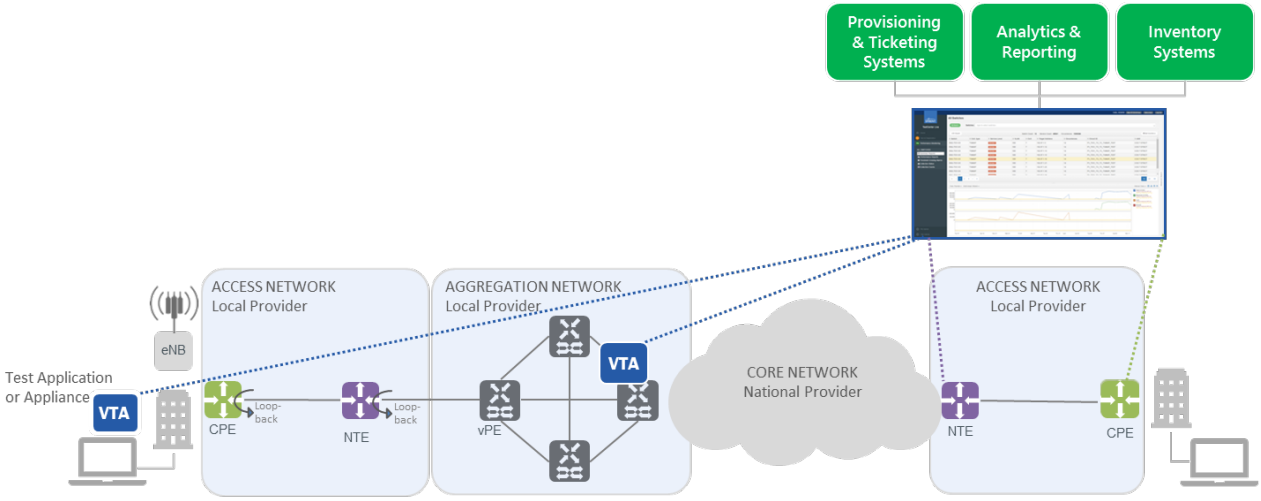

Figure 6 – Automation of End-to-End Troubleshooting & Fault Resolution

4. Integration of Systems with Service Assurance Test Controller

Having a single interface that controls all tasks simplifies the process of deploying, onboarding, operating, and maintaining services. Instead of applying a manual “swivel-char” approach the management of multiple systems from multiple locations, dependent systems can be integrated within a single Service Assurance Test Controller enabling automated ticketing and reporting and provide a complete “zero-touch” solution to provisioning and segmentation.

This also allows for a much more holistic approach to fault isolation and troubleshooting. This solution can automatically segment what area of the network the fault resides and automatically include this information in the trouble ticket which reduces time to repair or prevents a dispatch altogether saving time and money.

For example. inventory records can be retrieved by the service assurance system automatically and integrated with the alarm, trouble ticketing OS, customer trouble ticket portal, all reducing the amount of time to identify faults, isolate faults in a repeatable manner.

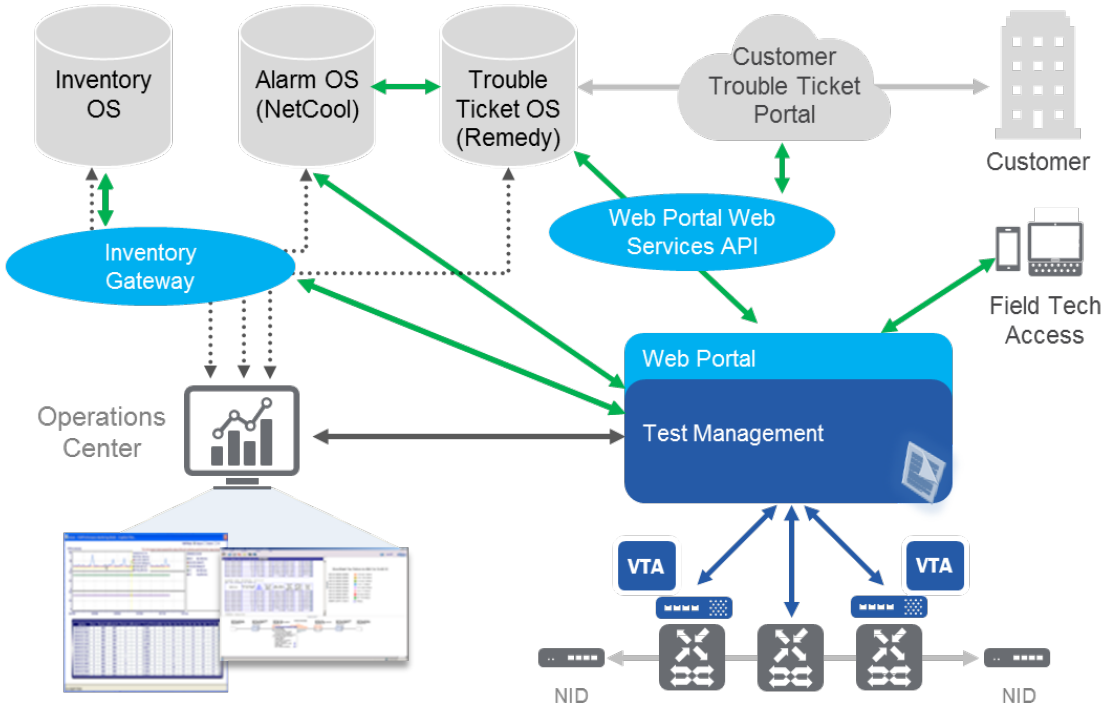

Figure 7 – Integration within a Single Service Assurance Test Controller

Integration of the service assurance test controller to all systems supporting an Ethernet service turn-up workflow enables workflow automation that can reduce test time more than 80% while also eliminating manual errors.

Table 1 – Test Controller Integration Enables Automation That Can Reduce Test Time by 87%

Task	Manual	Automated
Inventory Query	1 min	10 sec
Validate Configuration	20 min	20 sec
Enable Loopback on NTE	1 min	10 sec
Add Test Agent / Appliance to Service	5 min	30 sec
Execute Service Tests	4 min	4 min
Return Service to Original Config & Validate	10 min	40 sec
Total Time	**41 min**	**5 min 50 sec**

5. Scalability to Handle Drastic Service Growth

As Metro Ethernet services continue to grow and virtualization efforts accelerate this growth, the scale of service deployments and changes in the network will be exponential. With surge in the number of services and the frequency of changes, it will be impossible to manage without a large increase in OPEX unless a centralized and automated system is in place that can scale to the magnitudes needed.

While the promise of such a large-scale network deployment is exciting, providers are will have more users than ever before and various types of SLAs, so they will need a controller with the ability to simultaneously have multiple interfaces to active new customers **and** perform continuous active monitoring for existing customers.

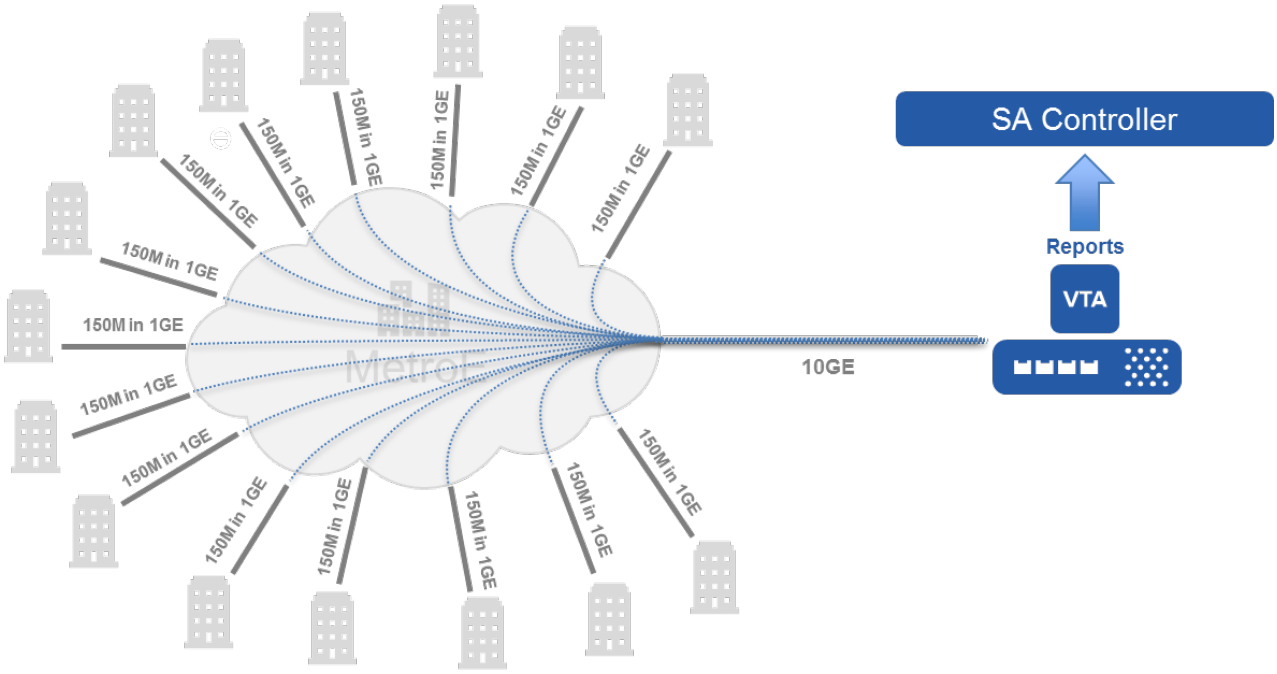

Figure 8 – Simultaneous Metro Ethernet Service Activation

Conclusion: Benefits & ROI

Spirent has worked closely with multiple tier-1 providers that have implemented automated service assurance systems and experience significant financial benefits. In one case, a tier 1 provider of Ethernet services implemented an automated service assurance system to monitor backhaul services provided to a mobile network operator. The mobile network operator experienced poor performance on the backhaul links and submitted a multi-million dollar SLA violation claim to Ethernet service provider. The Ethernet service provider could use SLA management and detailed diagnostic data from their service assurance system to prove the root cause of the SLA violation was in the mobile operator's network, saving millions.

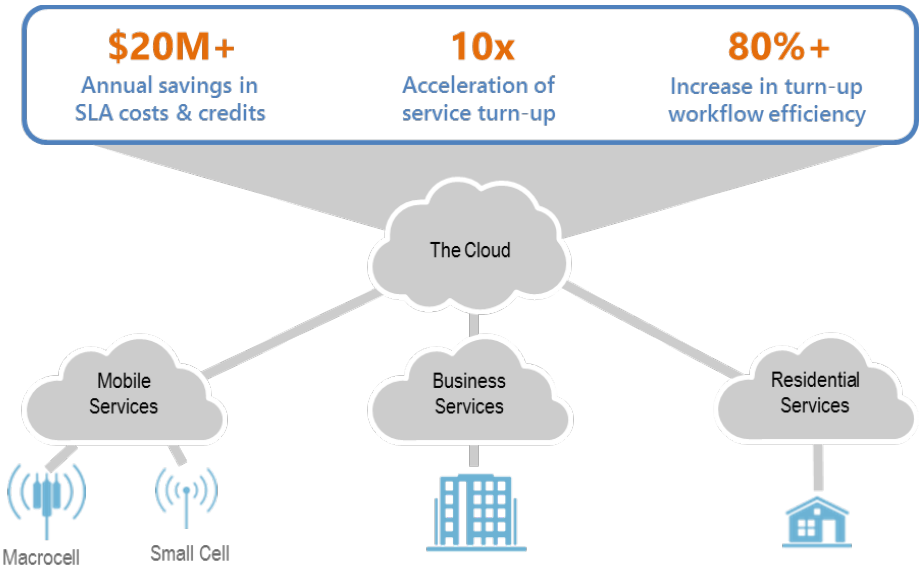

Figure 9 – Automated Service Assurance Delivers Significant Benefits.

In another case, a mobile network operator needed to roll out thousands of small cells and activate backhaul links for each of these new sites. The operator implemented a service assurance system to automate service activation testing of backhaul. As a result, the operator was able to accelerate the launch of small cells by an order of magnitude, from 100 to more than 1000 cells per week. In addition to improving the speed of deployment, the operator used automation to improve the efficiency of their activation workflows by 80%, enabling them to increase the rate of deployment without needing to add any additional resources to the activation teams.

As providers adopt NFV and SDN technologies, network configuration become much more fluid and dynamic. Workflows such as turn-up verification, SLA monitoring and issue resolution must be automated, as manual techniques simply won't run fast enough to keep up with network changes. In addition, since physical networks will persist for years, service assurance will need systems that unify these workflows across hybrid physical-virtual networks. As a result, automated service assurance is in the process of transforming from a highly beneficial, non-mandatory capability to an essential requirement.

Abbreviations

AAV	Alternate Access Vendor
SDN	Software-Defined Network
NFV	Network Functions Virtualization
PM	Performance Management
SAT	Service Activation Test
SLA	Service Level Agreement
TWAMP	Two-Way Active Monitoring Protocol
VTA	Virtual Test Agent

Bibliography & References

IETF RFC 5357: Two-Way Active Measurement Protocol (TWAMP), October 2008 (https://tools.ietf.org/html/rfc5357)

Technical Specification MEF 48: Carrier Ethernet Service Activation Testing (SAT), October 2014 (https://mef.net/Assets/Technical_Specifications/PDF/MEF_48.pdf)

Technical Specification MEF 46: Latching Loopback Protocol and Functionality, October 2016 (https://wiki.mef.net/display/CESG/MEF+46+-+Latching+Loopback+Protocol)

