Whitepaper

November 2021

Assuring service quality in the cloud and 5G era

Using Active Assurance to test across distributed networks

Author: Patrick Kelly with Grant Lenahan

In partnership with

JUNIPER NETWORKS

Appledore RESEARCH

Published by Appledore Research LLC • 44 Summer Street Dover, NH. 03820

Tel: +1 603 969 2125 • Email: info@appledorerg.com• www.appledoreresearch.com

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Appledore Research LLC independently of any client-specific work within Appledore Research LLC. The opinions expressed are those of the stated authors only.

Appledore Research LLC recognizes that many terms appearing in this report are proprietary; all such trademarks are acknowledged, and every effort has been made to indicate them by the normal USA publishing standards. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Appledore Research LLC maintains that all reasonable care and skill have been used in the compilation of this publication. However, Appledore Research LLC shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising because of the use of this publication by the customer, his servants, agents or any third party.

Publish date: 11/1/2021

Cover image: Photo by Patrick Kelly

CONTENTS

Executive Summary

Assuring quality of service in the cloud enabled network era is vital due to much more dynamic workload clusters spanning many more network domains. Delivering a high-quality experience will require more proactive testing and monitoring of virtualized network functions both within and outside the control of the telecommunication operators' network. Two out of three problems that occur today in an operator's network are reported by the customer and not identified by network operations. This leads to high churn rates and poor customer experience.

5G and cloudification will increase the complexity of the network architecture and operation's ability to respond effectively will expose weaknesses with existing tools and workflow process. The ability to offload reactive manual testing and augment passive monitoring is critical to avoid overloading the call center. The inherent issue with high touch reactive problem resolution is isolating problems quickly.

As networks become more distributed the ability to anticipate service impacting events is essential. Practitioners have a wide set of tools to help assure services but unfortunately some of these tools were developed for networks built to support fixed physical networks, not virtual software enabled networks of the future.

The focus of this white paper will evaluate more modern approaches to assuring high levels of service availability and performance. It is critical to maintain high levels of service quality not only within the operational domain of the service provider but also to extend this support across partner networks and 3rd party suppliers beyond the boundaries of the operator's domain.

This paper will take a perspective on how to validate new services and proactively resolve problems more efficiently in a dynamic modern cloud network. Active assurance is a newer approach to providing network operations and service operation centers with the tools necessary to measure and accurately report key network performance metrics.

The paper will evaluate an ideal service assurance solution architecture for operations in the cloud and 5G era and a comprehensive method for proactively pre-testing throughout full lifecycle management. The outcome of this approach will yield lower operational cost in different deployment models.

Key areas of focus will be:

1) Service quality visibility being extremely difficult to achieve because of the rate of network changes in 5G and cloudified networks where traffic transits partner networks, the Internet and clouds not owned by the service provider

2) Where device/network-centric data collection and aggregation by performance monitoring and network analytics solutions are falling short and where active assurance plays a role in augmenting existing solutions

3) Why the active assurance test agent approach is light-weight, cost-effective and easy to deploy in cloudified networks

4) Gradually implementing active assurance and growing to cover automation processes

5) Use cases over the operational lifecycle

The Quest for Quality

The telecommunication industry invests billions of dollars each year in labor and capital expenses in its quest to provide high availability and network reliability in its communication infrastructure. Unfortunately, these investments have not yielded improvements in Net Promoter Score (NPS). In fact, NPS has declined over the past several years published by independent NPS benchmarking agencies. NPS measures the loyalty of customers to a company.

The market for service assurance solutions consists of fault and root cause analysis tools, network and application performance monitoring tools, passive probing solutions, and drive testing. These solutions worked well supporting earlier technologies that can best be described as hardware centric nodes with static connections. The existing toolset helped to isolate problems and determine service impacting events. In most cases service assurance solutions were reactively used either on-demand or in a semi-automated process. This approach has some obvious limitations in managing the modern 5G, edge, and cloud infrastructure. Cloud native deployments dynamically scale where network functions are distributed in the network. Network functions move from being macro-monolithic and hosted on a single platform to highly distributed micro services deployed on VMs or containers.

As applications become more distributed, and in some cases latency sensitive, the workloads in the network shift in real time to meet user demands. The current workflow processes and the tools needed to support end to end service quality lifecycle management fall short in providing network performance in a modern network.

Assuring services requires a different approach to deliver high quality services in the cloud and 5G era. Assurance functions in this new modern network must be more automated and actively deployed in the network. Visibility of network traffic must be across technology domains and measure data flows from layer 2 through 7. Validation of QoS in a network slice or SDWAN is essential for business-critical applications.

Cloudification of the Network Requires a Re-think on Testing and Service Assurance

The cloudification of the network is a disruptive force in the network. It promises to deliver enormous economies of scale. At the same time, it brings with it increased complexity. 5G will increase problem resolution times by a factor of 10 compared to LTE deployments for root cause detection. The explosion of new protocols, densification of the RAN, and virtualization of the core network alone have the potential to overwhelm network operation teams.

The cloud and 5G era bring with it continuous software releases. This includes software embedded in the network and application releases. The frequency of software updates and lack of coordination across the diverse supplier chain will result in interoperability glitches. Testing, validation, and assurance are key inputs to the Continuous Integration/Continuous Deployment (CI/CD) model. CI/CD is an IT process workflow that automates software development and deployment. It differs from classic telco release models which follow more of a waterfall development process. The ability to rapidly test and validate operational readiness for a diverse collection of suppliers in the infrastructure is critical.

The telecommunication industry is facing a critical shortage of skilled IT workers. The scarcity of skilled staff combined with increasing complexity to operate and maintain services in the cloud network will jeopardize the CSPs ability to provide the customary Five 9's of service availability. It will force many

network engineers and operations staff to rethink how to test and assure the new services in the future communication infrastructure.

The cloudification of the network requires both new management tools and processes to achieve the benefits of cloud scaling. Agile service delivery and assurance radically changes how services are tested and assured as workloads become more distributed. Workloads will move dynamically to support demand scaling in/out in shorter timeframes. This obviates the need for planned deployment of dedicated fixed monitoring points, and in fact makes it impossible to locate precise points of monitoring.

Virtual probes will move with workloads at the edge closer to the UE and access points. Edge computing and the distribution of workloads will require more network visibility for service assurance and customer impact analysis.

Cloudification of the network will drive changes in how testing, measurement and service assurance systems will be deployed. The need for fixed dedicated tap points is becoming less relevant in the cloud infrastructure.

The key drivers for improvements in assuring services in the modern network era include:

- Market disruptions to support new business models in the cloud network
- Support for 5G, edge, virtualization, and distributed network security technology upgrades
- New methods to accelerate the turn up and testing of services utilizing techniques such as active assurance
- Investment in network automation tools to overcome complexity of densification in the RAN and dynamic workloads in the access, edge, and core networks
- A shift away from point tools to more multi-domain testing and assurance solutions
- Prioritization of tickets on the subscriber quality of service and less on network events
- Support of the shift in architecture for application and service aware security and connectivity

The Paradox of Assuring Services Across Technology and Geographic Boundaries

Until recently many CSPs built and operated their own communication infrastructure enabling CSPs to launch and manage all aspects of services with full control. The emergence of public and private clouds constrains the CSPs ability to gain full visibility of services that exits its network at the partner peering point. As enterprises move workloads from their private network to the cloud, visibility beyond the peering points will be difficult if not impossible to achieve with the existing performance management tools.

The current investment upgrade cycle required to deploy 5G, edge computing, and public cloud infrastructure technology further complicates the CSP's ability to gain visibility into network performance and service delivery. The core, aggregation and radio networks will be virtualized. Software functions will be more distributed resulting in massive increases in data flows to provide voice, video, and data connectivity.

Edge Cloud is effectively the migration of data centers and local processing to the edge of the network. Functions at the edge are inherently software on virtualized hardware. The CPE moving to the edge is already proving this out. The dynamic nature of the edge layer will respond to changing needs of the application layer. The Edge model is not well suited for classical network probe-based solutions because network functions will be encapsulated into micro services. This includes monitoring which will be deployed onto the virtualized infrastructure.

The edge environment is also increasingly being dominated by the web scale players. This will create gaps in the ability of CSPs to determine performance issues and isolate problems for services that cross into the cloud or partner's external network.

Finally, cloudification, both in public cloud and at the edge, changes the nature of what it means to scale and be resilient. Applications are no longer designed on highly resilient vertically integrated stacks. Instead, applications are deployed on large numbers of individually un-resilient infrastructure components, with scaling and resilience achieved by the application over that un-reliable infrastructure. In this world "the best" most efficient application can lose to the "better" lower cost alternative that can scale with cloud. The best dedicated probe may lose to the better scaled, "cloud mature" network performance monitoring tool.

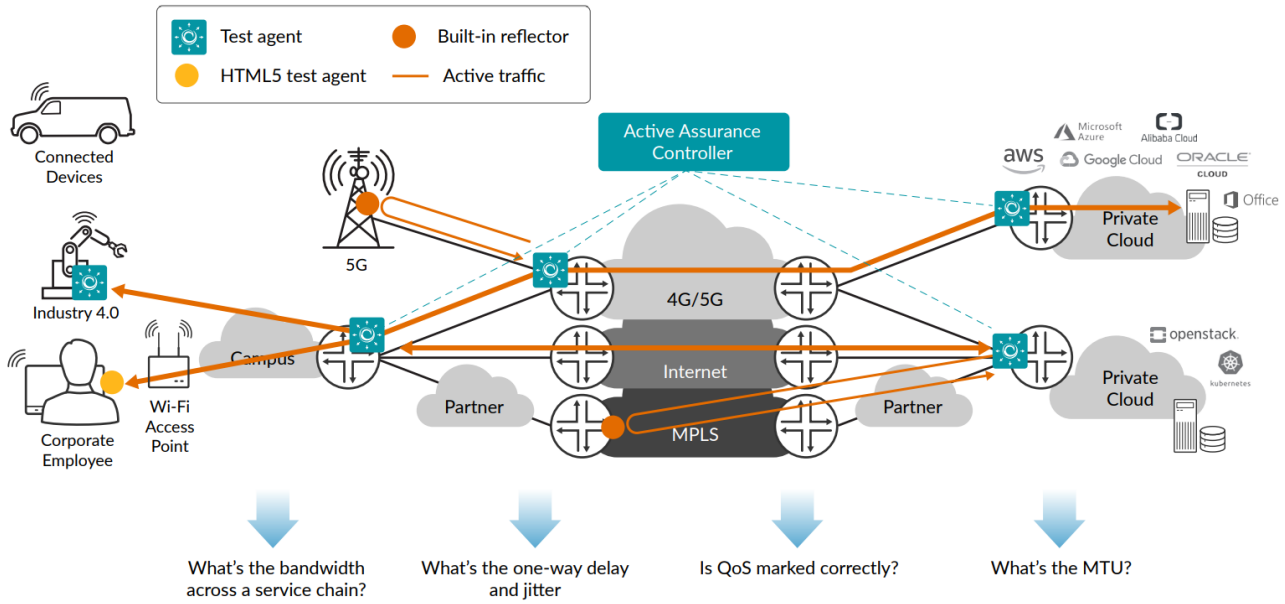
How do CSPs assure high quality of services over a large vast communication infrastructure cost effectively? One area gaining acceptance is active assurance because it is optimized for the new technology and provides a lower cost deployment model to traditional service assurance solutions.

Active Assurance

The cloudification of the network will drive changes in how testing, measurement and service assurance systems will be utilized in the optimization and operations of the network. The need for fixed dedicated tap points is becoming less relevant in the cloud infrastructure. Instead, the market is moving towards active testing of the service. A test controller can model the service and identify the key performance metrics required for each type of service. The controller coordinates with virtual test agents to run simulated transactions using synthetic layer 2 to 7 traffic which can then provide the operator with the confidence in both pre- and post-deployment phases.

Active assurance simulates the performance metrics necessary to deliver a consistent service both inside and outside the network control domains of an operator to provide a high degree of confidence on actual data plane traffic performance. This technique is superior to older performance monitoring systems that poll, collect, and infer network performance characteristics. It is also essential to manage and monitor complex services such as network slicing that deliver customized service quality tunnels to individual users and applications.

Figure 1 Active Assurance Controller



Source: Juniper Networks

Active assurance supports processes like continuous integration and development. As services are spun up in minutes and upgrades occur weekly, network operators must be confident that services perform flawlessly. Data must be captured, processed, and analyzed in short cycle times. It must then coordinate with the intent of the network and policies defined by the user, application, and service.

AIOps and Active Assurance

Active assurance provides valuable input into functions performed in the AIOps layer. The abundance of high-quality data, advances in computational processing, and sophisticated machine learning models is reducing both the cost and accuracy of applying AI compared to conventional hard coded methods. The high value data from active assurance systems is the fuel that drives AI engines and delivers the business outcomes that until now were not possible. Attempting to deploy AI even 5 years ago was not economically feasible because of limited data sets, higher cost computing, and inferior ML models to conventional statistical regression techniques. In short, it was difficult to justify the economic benefits until now.

The value of AI is that it uses data to discover patterns, and then predict outcomes more reliably than current methods. The power of AI is that it is constantly improving its learning algorithm, using a technique called back propagation that changes weights in the hidden layer, to achieve higher levels of accuracy.

The tuning and optimization of the network is quickly shifting from being controlled by highly skilled craft technicians to becoming a fully autonomous network. The radio interface performance parameters combined with virtualization of network functions in the core network will overwhelm the

largest most capable mobile operators in the world. Appledore Research contends that if 5G is deployed with existing operational processes and systems environment, operational costs will balloon and on a long-term basis is not sustainable.

Previous generations of mobile network have fundamentally been about connecting handsets with centralized monolithic carrier grade applications and the internet, with the mobile network acting as an access technology between handsets and these central applications. 5G will be the first generation of mobile connectivity that is about connectivity to cloud applications and these cloud applications now have the potential to be distributed within the network.

In the 5G network it is possible that a provider may want to support a low latency application in a robotic manufacturing facility which demands recurring and rapid changes to factory production demands. The desired network state and associated KPIs must be captured in near real time to initiate new services, move workloads, or re-route network connections if the service is impacted. Active assurance can be utilized as a precondition for machine learning to help build a service profile and identify the data parameters. AI is dependent on the ability to collect and process large amounts of telemetry data to identify patterns and determine if the service is operationally “green”. Any service impacting event should drive an event trigger to the network orchestrator or service controller.

Applying active assurance with AI can facilitate autonomous operations as cloud business models take hold. The ability of the RAN-cloud to self-manage will be necessitated by the application of intelligent algorithms and real time data processing supported by assurance systems. Machines will outperform human experts’ ability to predict what must be solved and therefore we need self-learning and self-training AI and ML. Initially we expect that ML “findings” may be checked and confirmed by human experts. Once they pass this review it will slowly be placed into automated production with simpler rules and search algorithms.

Shifting Sands from Reactive and post-mortem analysis to proactive assurance

Passive probing focuses on what, when, and why of events in the past. It helps to provides a more in-depth forensic analysis of actual network communication that occurred in the past which is useful for troubleshooting but lacks any real time focus on service impacting events.

Active assurance is designed to be proactive and drive changes in the network if capacity is being reached or delays are occurring in latency sensitive applications. The focus of active assurance is on the data plane where users consume the services, irrespective how and where they are produced.

Understanding the performance of applications must be understood in the entire data stack (layer 2 -7) and support the data flow that transits multiple technology domains.

The best practice approach for the cloud era must change workflow processes to support full life cycle management. As we noted earlier software and services are continuously developed. The testing and assurance of services is not an afterthought. Instead, it is integral in the development and pretrial test phase through the life of the service. Appledore has developed a framework for how we expect to see

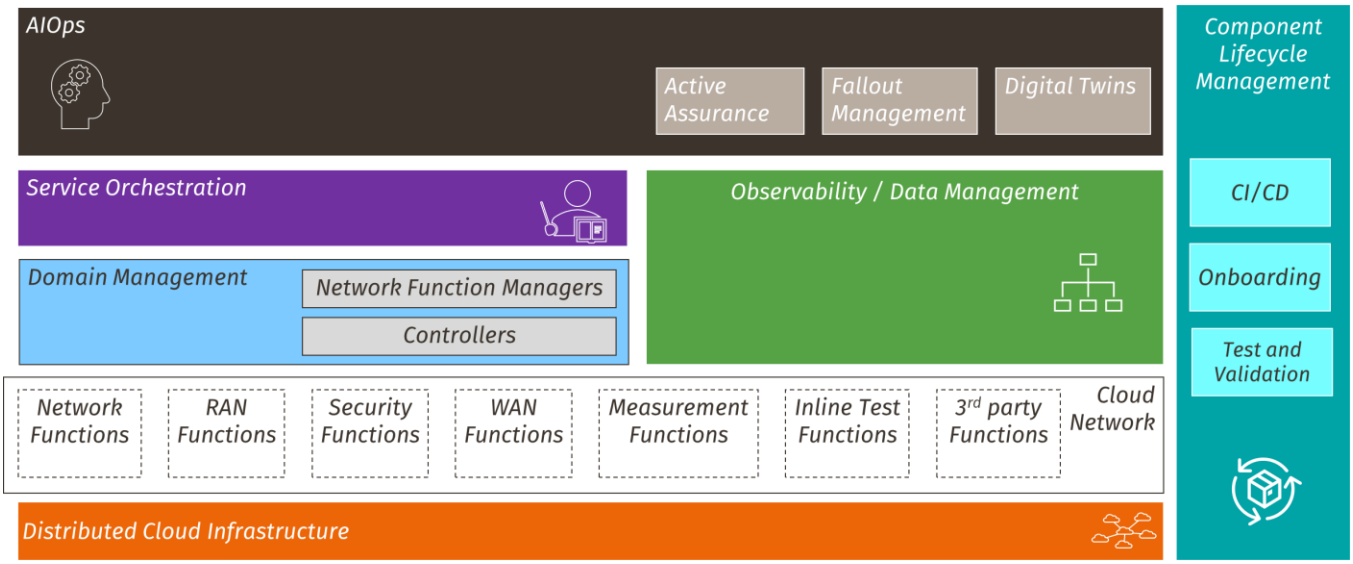
network automation software deployed in the cloud era. For more on this topic please see *"The Automated, Actively Assured Service Lifecycle"*.

Applying Active Assurance in the Modern Cloud Network Era

As the modern network evolves so must the management systems. Automation and active assurance complement the new construct in the cloudification of the network.

Figure 1 provides a view from Appledore Research as to how we see the network automation software market changing to support the modern network.

Figure 2 Framework for Managing Modern Cloud Networks



Source: Appledore Research

Network functions are the building blocks of a cloud native infrastructure. Other important functions include domain management which interface with the cloud infrastructure in real time. Controllers for instance are used to configure policy parameters which are enforced in the network at each node in real time. Service orchestration defines intent in the network and interfaces directly with domain managers and takes input from AIOps on the state of the network. Component lifecycle management is a function that monitors and measures the overall performance of services and applications. AIOps will use the abundance of data generated within the network to train and enable the machines to learn and detect network anomalies. In many cases this can be done faster, cheaper, and with more accuracy than existing tools. Each of the components both complement and performs critical functions to automate task that in the past were performed by highly skilled staff in engineering and operating the network.

The modern era cloud network will push the limits of the largest technically proficient operators in the world. In short, the cloud era network cannot be manually configured, monitored, and tested by human experts. Cloud applications are on-demand and scale up and down sometimes in short intervals. Workloads move around. New releases of software arrive daily. The network will need to be managed in real time and the potential permutations of data flows to deliver a service will increase 10-fold.

To successfully deliver high quality service in the cloud era network, CSPs must automate more of the mundane task in operating the network. Active assurance provides framework to continually test, validate, and assure services through the entire lifecycle.

Buyers Guide to Active Assurance for Life Cycle Management

To achieve full visibility of a data session, active assurance solutions should provide out of the box capabilities to test packet transmission from the data layer 2 through the application layer 7 in the OSI model. The use of synthetic packet transmission to test for reliable transmission confirms and validates the delivery and operation of the service life cycle.

A common business problem that CSPs will face in the cloud era is the ability to test and validate services in external networks outside their control as is the case with cloud providers. NNI peering points create a demarcation where the CSP may lose visibility of how the service is performing potentially jeopardizing the service level agreement.

Active assurance generates packets that are routed the same way as user-initiated traffic. As a result, active assurance enables CSPs to instrument and measure the complete network path including networks not owned and managed by the CSP.

A major challenge for mobile CSPs deploying 5G services is quality of experience. Allocating a network slice in the 5G network is a powerful technique to assure network quality and separate high bandwidth traffic and ultra-low latency sensitive applications. Providing 5G slice assurance can be achieved using active assurance solutions. For more on how this technique can be applied please refer to *IEEE An Integrated Instrumentation and Insights Framework for Holistic 5G Slice Assurance*.

Implementing Active Assurance

The commercial use of active assurance technology is available today. The components include:

1) Lightweight agents deployed as virtual machines, containers, or packaged as a turnkey appliance
2) A control center with APIs to orchestration systems to enable automation of service turn-up and sustained performance of the service

When started, the active agents use four different methods to simulate the test harness to measure and monitor the performance of the network.

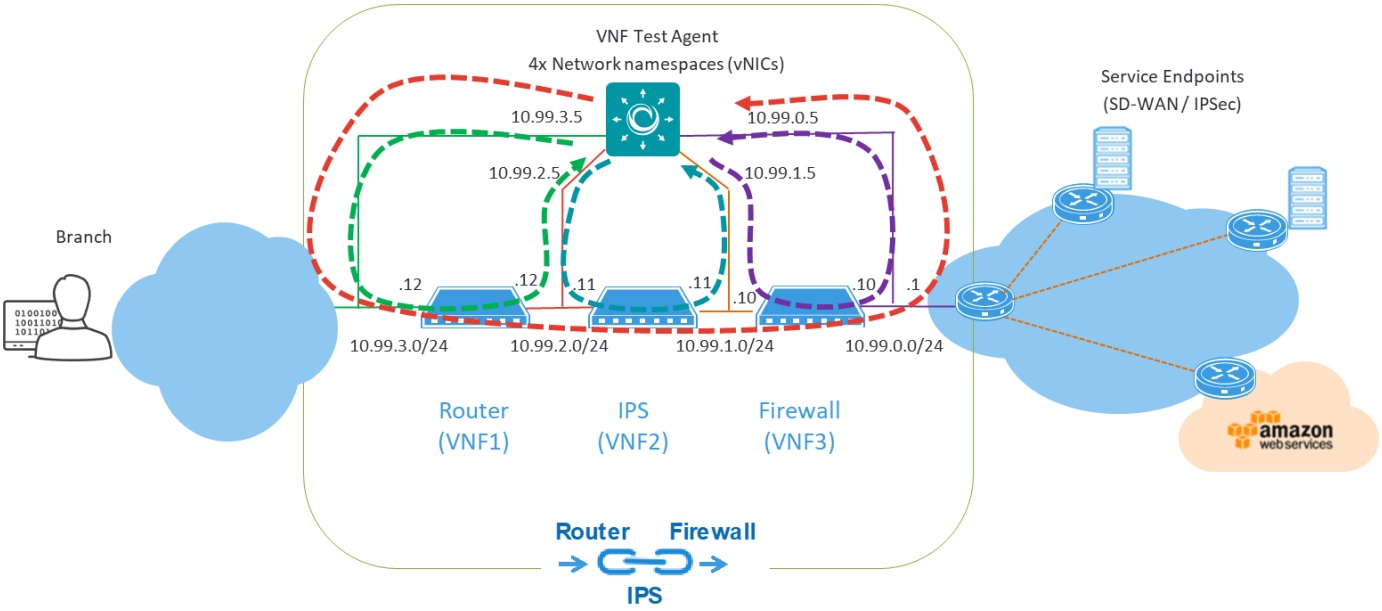
1) The test agent injects traffic into the network to another test agent and measures how the network performs between both agents.
2) Reflector technique which sends traffic towards the network element such as a router. TWAMP and ICMP techniques like traceroute are different examples.
3) Perform application request towards servers. This will do DNS lookups, http requests etc, to validate network applications as well as SaaS applications like Office365.
4) Test all the way to the end user using HTML5 browser test harness. This helps to identify issues with the local network and/or Wi-Fi and determine if problems exist in the customer premise or partner network.

Agents can be run continuously injecting a small amount of traffic on the network. This 24x7 monitoring can provide the operator with information on how the network is performing on a permanent basis. Thresholds

can be set to alert the operator of potential SLA violations. Automated troubleshooting sequences can be achieved by initiating on-demand synthetic traffic.

Figure 2 provides data flows across each network function performed by the active agent. This data flow can mimic the service chain flow of a live session and report back performance metrics for each software node in the chain. Any unsatisfactory performance thresholds can be isolated to the specific link in the service chain.

Figure 3: Sectionalizing the Service Chain



Source: Juniper Networks

Use Cases

Backhaul Network Performance

The challenge in mobile backhaul and IP core networks is determining if all routing nodes are satisfying the load and performance metrics required to meet service quality metrics. The technical challenge is isolating low level problems that may be impacting higher layer services. It often results in long duration substandard performance that is difficult to resolve.

The underlying problem is often a misconfigured router that impacts service quality or high bandwidth traffic burst over a short period of time. These problems can be resolved quite easily with active test agents and reflecting simulated traffic using the Two-Way Active Measurement Protocol (TWAMP) protocol.

The benefits of active assurance using TWAMP include:

- Testing and monitoring can be achieved end-to-end without using a dedicated testing device.
- Test timestamps provide high degrees of accuracy on two-way or round-trip metrics.
- It is a robust method to check service-level agreement (SLA) compliance.
- Pinpointing the problem area and dramatically lowering MTTR.

Edge Network Performance

In the modern cloud era network the distribution of network functions is implemented using a Cloud-Native Network Function (CNF) which runs inside a Linux container. The network becomes much more complex because software network functions are distributed and across different network technology domains. This often results in poor visibility using existing toolsets.

The use of active test agents in this scenario can be deployed to validate pre-test performance prior to the launch of the service. This is frequently the case in the environment where continuous development is the norm. Active test agents can be deployed as a container in the edge to measure performance of each network function.

Multi-cloud and data center interconnect

Determining performance outside the CSP network domain where the peering routers act as a demarcation point is a challenge for CSPs that provide services on a regional and in some cases global basis.

Test agents can be deployed in a public or private cloud. In this instance complex routing and security policies exist between clouds and the test agents can provide visibility and validate communication in this type of shared infrastructure.

The benefits of active assurance in this use case are the ability to troubleshoot end to end performance much more quickly for service impacting events outside the CSP domain.

End user performance

The use of active assurance can be utilized to isolate and measure performance at the end user. This technique can be applied to any device using HTML5 web browser. Testing can measure bandwidth, packet loss, and jitter. This is an ideal troubleshooting tool to isolate problems with VPN access, network address translation, and proxy gateways.

Conclusion

CSPs should design future assurance solutions to scale based on dynamic workloads and data that flows across many technology domains. Some of these technology domains will reside beyond the geographic boundaries of the CSP.

Current methods of testing and assuring services are both expensive and inadequate. As network functions become more distributed, network observability declines using current tools. Therefore, CSPs must adopt a new approach to gain increased visibility. The active agent solution provides a cost-effective solution that expands visibility both inside and outside the domains controlled by the CSP.

The robustness of the active assurance solution allows CSPs to:

1) Gain increased visibility of how services are performing both inside and outside the operator's network
2) Validate service performance confidence prior to the deployment of services
3) Monitor and isolate service impacting events at discrete points in the service chain
4) Deliver a cost-effective test and monitoring solution in a cloud native network

In partnership with

Insight and analysis for telecom transformation.

@AppledoreVision

Appledore Research

www.appledoreresearch.com

info@appledorerg.com

+1 603 969 2125

44 Summer Street Dover, NH. 03820, USA