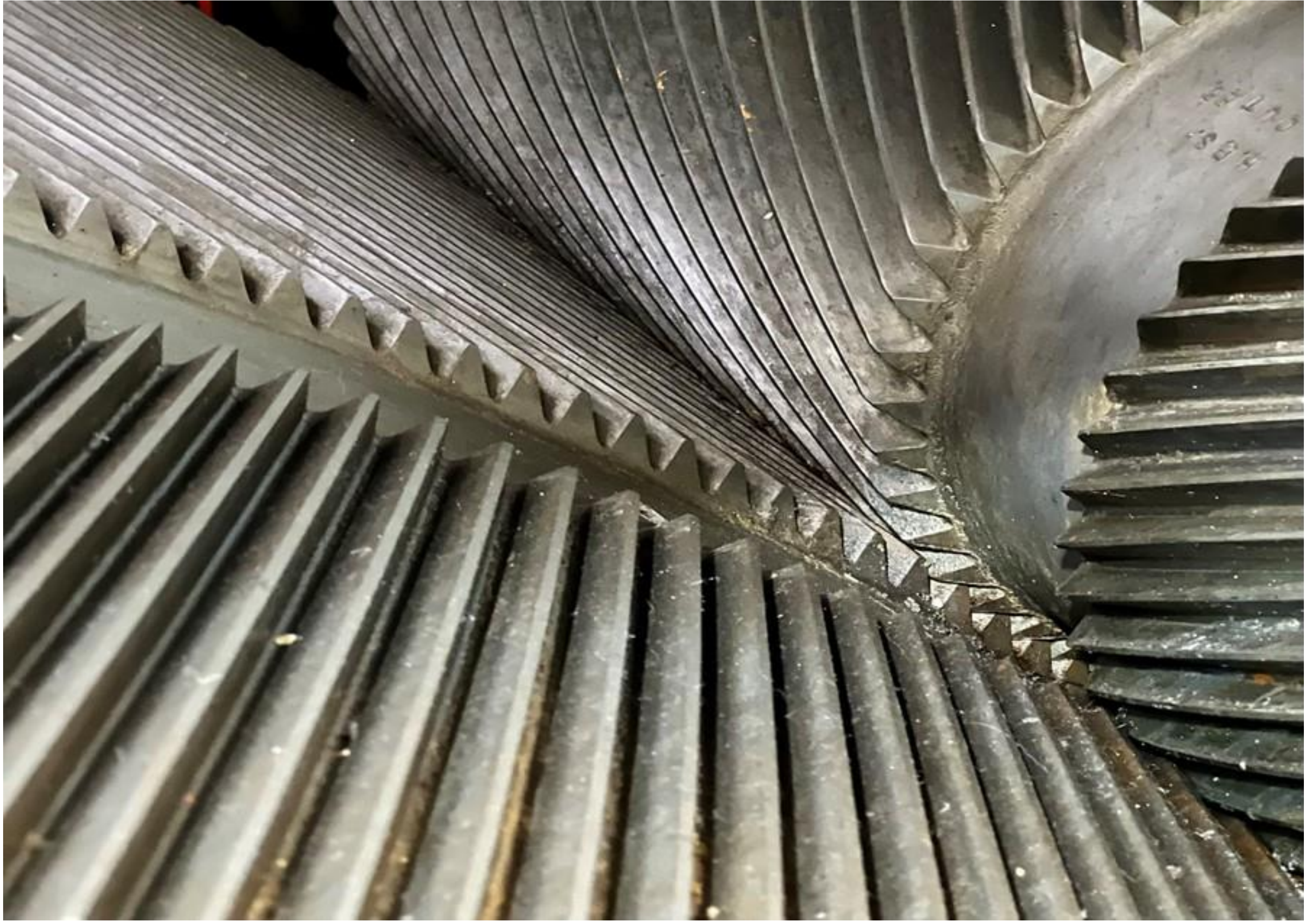
Whitepaper

March 2023

# Intent-Based Networking

## Automated Assurance's Critical Success Factor

Author: Patrick Kelly Principal Analyst Appledore Research



In partnership with

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 16 March 2023

Cover image: Photo by Patrick Kelly

# CONTENTS

# Executive Summary

The telecommunication industry is facing its own innovator's dilemma moment.

The global telecommunication market is undergoing multiple technological transformation. This includes cloud computing, network virtualization, disaggregation of the radio access network, network automation, and leveraging applied AI using robust machine learning algorithms. A key characteristic of these enabling technologies is more distributed software-based feature releases onto commodity-based hardware that ultimately drives down the cost per bit to deliver voice, video, and data services.

CSPs can start accruing the benefits of the programmable network if automated assurance is deployed as a critical success factor of network automation. Network automation must be thought of as more than network orchestration of services or domain level network controllers.

To succeed with intent-based networking, CSP must have a plan as to what success looks like. Critical success factor for intent-based networking must drive a business outcome such as reducing MTTR by 50% or delivering a ten-fold improvement in service order fulfillment. Without automated assurance I argue that you can't achieve intent-based networking.

Many long-held beliefs about how to plan, deploy and operate a network will require a rethink on how to achieve it as the network becomes more distributed and complex to operate. This paper will evaluate why automated assurance is critical in supporting cross domain service orchestration. It will also explore the techniques of measuring layers of the distributed network to validate intent based networking.

Network automation cannot be underestimated in the race to capture new markets, drive an order of magnitude change in operational efficiency, and improve profitability in an increasingly commoditized communication industry. Any delays in transforming CSP operational workflows to leverage these disruptive technologies will open the door to competitors who will take market share and further disintermediate the vast communications infrastructure where hundreds of billions have been invested over the past decade.

We have seen this scenario play out in the first wave of cloud-orchestrated infrastructure. After AWS launched in 2006, CSPs were in a race to build out massive data centers, first regionally and then globally. Some CSPs made acquisitions, and others built their own. At the same time, Microsoft, IBM, Google, and others also entered the market.

The hyperscalers architected and deployed IT software tools like Ansible and Python to automate and orchestrate advanced workflows across the data center infrastructure, network, and cloud. Fast forward to today, and we can declare that AWS, Azure, and GCP have emerged as the winners in the cloud market. Their ability to orchestrate and improve efficiency using data, automated analysis, and monitoring was a critical component necessary to establish superiority in the market.

We are now entering the second wave of intent-based networking. This is the ability to define a service level and assure that the network can maintain that state regardless of anomalies or service-impacting events. This requires near real-time awareness of how the network is performing and the ability to isolate root cause by understanding the relationship of each layer in the technology delivery stack.

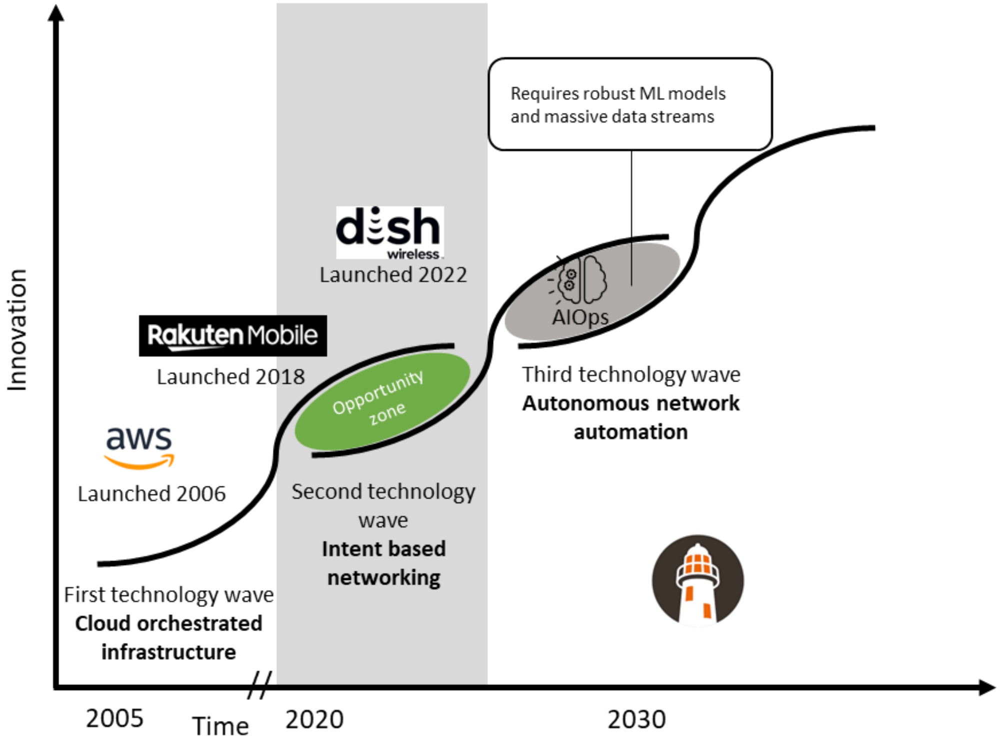
Intent can only be achieved with near real-time telemetry analysis that can inform adjacent policy and orchestration systems that coordinate with domain-specific network controllers.

This paper will examine the current state of the market, reveal best practices in applying intent-based networking, evaluate use cases, and evaluate Cisco’s strategy in helping customers reach the second wave of telco network automation with automated assurance.

## Introduction

We are entering the age of enlightenment. CSPs can choose the status quo or embrace the marvelous technology innovations on the horizon. When AWS launched in 2006, it brought on-demand cloud computing and storage to the market at a fraction of the cost of conventional IT options. The game changer was that AWS provided a fast, flexible, convenient way to rent cloud computing resources. It did this by automating the management of AWS cloud and exposing self-service portals with highly flexible APIs to empower customers, suppliers, and application developers to harness the power of the AWS cloud. This was the first technology wave we classified as the cloud-orchestrated infrastructure (figure 1).

**Figure 1: Network Automation Technology Waves 2005 - 2030**



*Source: Appledore Research*

This market is mature and is primarily dominated by three large hyperscalers, AWS, Azure, and GCP, which control 65% of the global market. Each hyperscaler provides the infrastructure and software to automate and orchestrate advanced workflows across the data center infrastructure, network, and cloud.

We are now entering the opportunity zone for CSPs. In this second technology wave the focus is on intent-based networking. It combines automated assurance as a support function to policy and orchestration systems.

## Innovation Wave 2: Intent-based Networking

Intent provides the network with declarative information on “what” is being requested, effectively disaggregating the “how” to systems that catalog, provision, and maintain it. For example, you can define the SLA without stating how to achieve it. This implies that the orchestration logic and availability of resources can find and implement a solution to the “SLA.”

Cloud-native networks already use intent-based methods, allowing telco operators to readily adopt leading-edge technologies and best practices. Intent can unleash order-of-magnitude improvements in cost and agility.

Appledore believes that over time, cloud-native automation, based on “good” intent, can reduce maintenance and re-integration costs by more than 50% since detailed logic and models do not update each time a related process, equipment, or software changes. This has been proven out with Google Anthos and Azure Operator Nexus solutions. Both provide end-to-end visibility with telemetry data flows and automated network configuration.

The rationale for intent is to reduce technical complexity, provide algorithms with greater flexibility, and reduce long-term operational costs. Using intent-based model definitions and intent-based orchestration and assurance, operators can expect to achieve:

- More hands-off automation.
- Flexibility in the face of congestion, failures, and other realities.
- Simplification of auto-healing and auto-scaling.
- Higher degrees of successful flow-through on orders, especially self-care orders, without expert human intervention.
- Vastly simpler service definition and, therefore, innovation.
- Reduced testing, maintenance, and integration costs.

The success of intent-based networking in the public cloud has demonstrated its value, but at the same time, it demands a radical change in operational workflows and management metrics. However, this change is necessary for telco operators to implement automated assurance and process automation.

Assuring services in a cloud-based environment requires operators to adjust their past methods and operating determinants to account for:

- Top down starting with customers to understand dependencies of services and resources.
- Real-time data flows to dynamically adapt to network requirements.
- Multi-domain transparency to facilitate greater operator situational awareness.
- Learning algorithms using AI/ML to predict future service states and dynamically reconfiguring the network to avoid problems by leveraging prior experience.

## Market Dynamics

CSPs face numerous challenges today, but none will be more impacting than transitioning to a cloud-native architecture. The massive growth and adoption of cloud services and the broad availability of cloud-centric APIs help to confirm the mainstream success of the cloud business model. These cloud service providers have spawned an equally robust set of vendors and integrators that support a cloud services industry that has come to dominate enterprise markets.

The cost-savings of cloud-based networks, plus the speed of service deployments, will be highly disruptive to incumbent operators. New entrants like **Rakuten Mobile** and **Dish Wireless** use a cloud-native-first architecture competitively, attempting to leapfrog existing service providers by building cloud-native operational and business support systems designed to be more dynamic and malleable to business conditions.

Migration to a cloud-based architecture has resulted in an innovator's dilemma for traditional operators. The innovator's dilemma, a business concept popularized by Clayton Christiansen, suggests that disruptive innovation is pivoting towards future customer demands. The trap is to maintain status quo in supporting the existing customer base and refusing to cannibalize parts of the business. To avoid the dilemma, CSPs must plan and execute the transition to newer more efficient business models and innovation platforms to secure their moat. Incremental innovation means incremental investment, allowing operators to become more agile in delivering new services with the benefit of a highly scalable programmable network.

## Automated Assurance delivers the promise of intent based networking

Automated assurance simplifies and reduces costs while introducing a systematic testing methodology that improves user satisfaction. Adopting automated assurance demands new thinking and process change.

Intent must span the entire service path, asserting network delivery expectations and requirements throughout the transaction. This requires expansive network observability. It must be multi-dimensional to include optical, IP, and backhaul. Instrumenting the network to become more proactive requires the right tooling not only within the operator's network but also outside the boundaries of it as multi-cloud networks become more prevalent.

CSPs are uniquely positioned to add end-to-end value, given their sizable footprint and transport experience. Now they need to prepare their operating environment with the software tooling to deliver on intent-driven, automated assurance.

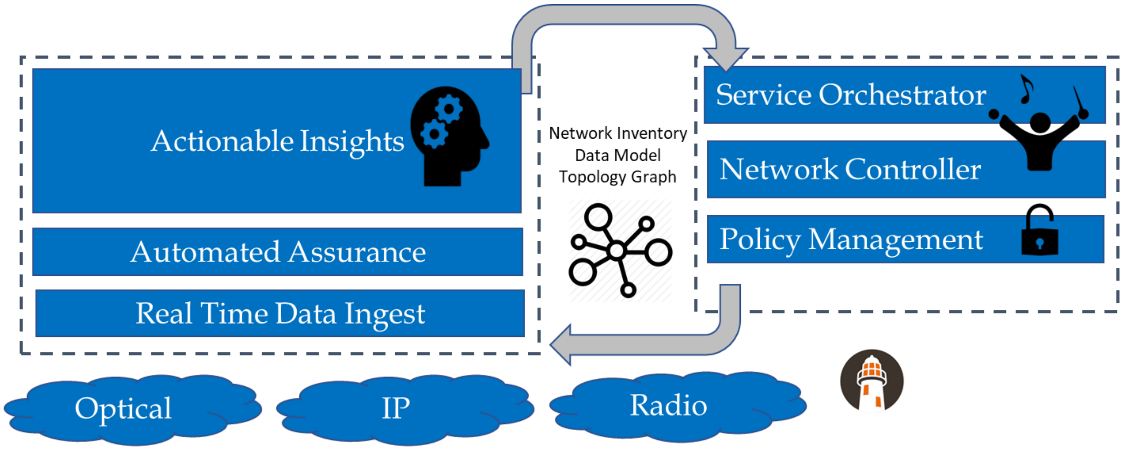
Enabling automated assurance for cloud services and cloudified network functions requires that assurance metrics and capabilities are designed, engineered and integrated within network automation models and implemented as a closed-loop process. Importantly, automated assurance requires operators to determine the level of assurance needed, what's possible within the context of their networks, and when to consider assurance operations at scale.

Figure 2 provides a visual graph of how we see the interplay of automated assurance and network controllers, policy management, and service orchestration in the modern operator's network operations. Automated assurance relies on real-time insights of end-to-end network performance. The resulting measurements can provide critical insights into current or impending service impacts.

The data management layer which is a shared resource combines network inventory, topology graph database, and a data model (i.e., YANG) to bind the assurance functions with the orchestration of services. YANG is a data management model that can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations. YANG is primarily used to model the configuration and state data used by NETCONF operations.

The data flow loop is a continuous process that measures optical, IP, radio, and other network performance metrics against the defined business service. If any resource fails to deliver the requisite performance values or the network performance is impeded, then a trigger event is generated. The trigger events can be supplemented with pre-processed and pre-analyzed performance metrics to give further context to the events. This generates an action usually handled by a network controller or orchestrator to reconfigure the network to maintain acceptable service level performance.

**Figure 2: Appledore Network Control and Automated Assurance**



*Source: Appledore Research*

There are several advantages to automated assurance:

- It is real-time, significantly improving operator situational awareness.
- It understands context by leveraging shared models, topology graphs, and inventory.
- It is universal and can transit multiple domains and multi-vendor deployments to accurately reflect end-to-end user experience.

Automated assurance promotes proactive responses to changing conditions in the network. It is an important input to better understand how the network is performing and whether it can satisfy the SLA metrics. Automated assurance is also adaptable and able to change as the network underlay changes in response to topology reconfiguration, workloads, and mobility of service and endpoints.

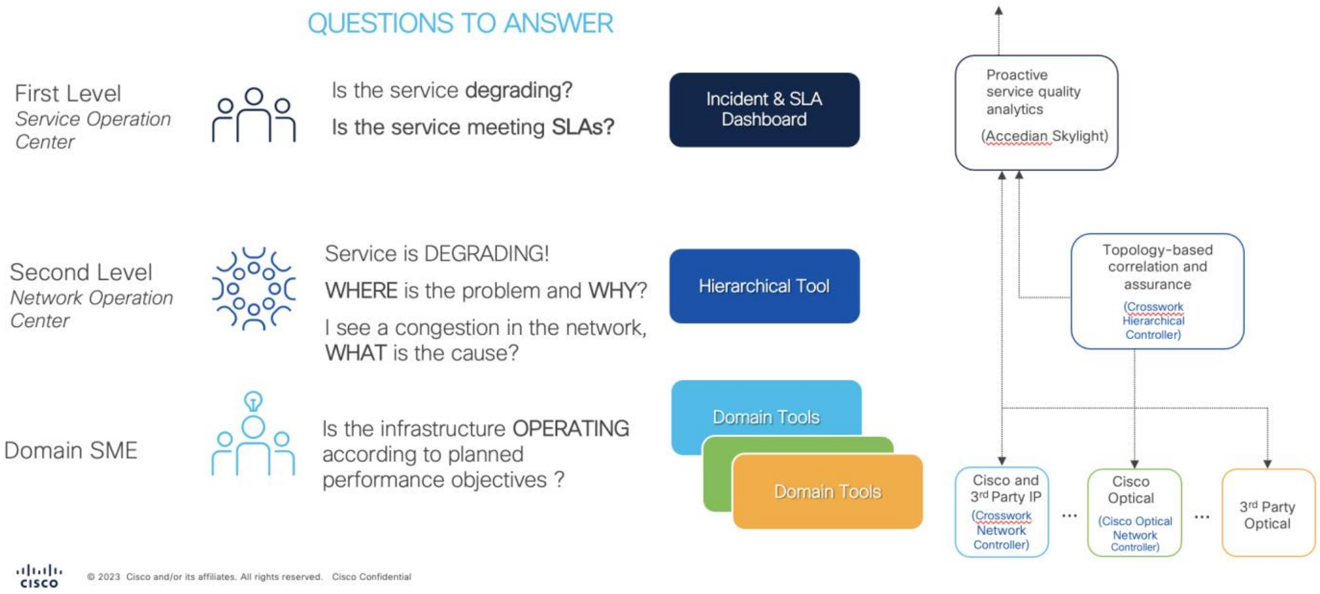
Intent-based networking is model-driven, capable of spanning a service or network function's entire life cycle and is perfectly matched to automate active assurance/test technology. With automated assurance, operators can reduce and even remove human intervention, making deploying new services at scale practical. Cisco's approach to automated assurance includes an integrated, open-standards-based set of use cases that allows operators to simplify their fulfillment and assurance processes and support their broader automation initiatives.

## Crosswork Automated Assurance Use Cases and Business Proposition

Cisco takes a top-down approach focusing on the customer. At a high level, Crosswork is designed to improve service visibility, provide more significant insights into how the network is providing service, and accelerate any actions required to address service-impacting issues. Crosswork automates many network functions and simplifies troubleshooting by providing operators with an integrated view of a disaggregated network. Cisco understands how operators monitor and manage network operations and has evolved the Crosswork platform to provide the tools to manage virtualized assets that meet negotiated service assurance requirements.

Crosswork takes a multi-layered top-down approach, reflecting the operational structure operators use to manage SDN domains and monitor network performance.

**Figure 3 Top-down Approach to Automated Assurance**



QUESTIONS TO ANSWER

First Level
*Service Operation Center*

Is the service degrading?
Is the service meeting SLAs?

Incident & SLA Dashboard

Second Level
*Network Operation Center*

Service is DEGRADING!
WHERE is the problem and WHY?
I see a congestion in the network, WHAT is the cause?

Hierarchical Tool

Domain SME

Is the infrastructure OPERATING according to planned performance objectives ?

Domain Tools

Domain Tools

Proactive service quality analytics
(Accedian Skylight)

Topology-based correlation and assurance
(Crosswork Hierarchical Controller)

Cisco and 3rd Party IP
(Crosswork Network Controller)

…

Cisco Optical
(Cisco Optical Network Controller)

…

3rd Party Optical

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

*Source: Cisco*

## Level 1: Service Operations Center (SOC)

The SOC focuses on meeting customer service levels. It requires high-level analysis and real-time alerts to identify valid threats to service levels. Cisco Crosswork collects performance data and state information across multiple domains and uses Accedian Skylight to present operators with a simplified dashboard reflecting top-level performance concerns that are SLA-impacting. Accedian's Skylight test and assurance platform delivers real-time analytics from test probes deployed throughout the network, collecting, and measuring performance data and KPIs for targeted customer services. Given Crosswork input, the SOC can determine when a service is degrading to where SLAs are being violated and take quick action, usually directing level 2 staff to take further action.

## Level 2: Network Operations Center (NOC)

The NOC is where operators use active network topology views to drill down and determine the source and cause of specific service issues. The Crosswork Hierarchical Controller gives operators a multi-layer topology view that can identify and isolate specific network issues or determine whether multiple issues simultaneously contribute to a specific incident. The NOC can use network-specific evaluation tools to decipher whether issues are confined to a single domain or span multiple domains. Once identified, the NOC can pass incident-relevant information to Level 3 staff to take further action.

## Level 3: Domain Subject Matter Experts (SMEs)

Each domain is managed by SMEs with dedicated tools capable of troubleshooting and resolving issues within their domain. Domains can include transport assets like the Cisco Optical Network

Controller and Crosswork Network Controller, service management from provisioning and monitoring service health, traffic engineering optimization, service metrics, and Element Management functions like device fault and inventory to provide deep visibility into infrastructure health. Using domain-specific tools, SMEs can identify components that adversely impact network and service levels and take immediate corrective actions.

Cisco has designed the Crosswork to support closed-loop operations, where information flows between different levels and presents a view that is appropriate for targeted decision-makers. Crosswork combines analytics that can pinpoint specific issues with heuristic decision models that determine an appropriate course of action. Level-appropriate toolsets are integrated so that operators can take appropriate action or added to an automation workflow that can accelerate problem resolution.

The benefits of combining real-time analytics and efficient process flows to deliver automated assurance are significant and can only be achieved by constructing an end-to-end, real-time, multi-layered, intent-driven architecture. Cisco Crosswork offers pre-packaged solutions to address automated assurance use cases. The solutions allow  operators to ensure customer SLAs while automating the assurance process, allowing them to cost-effectively scale network services.

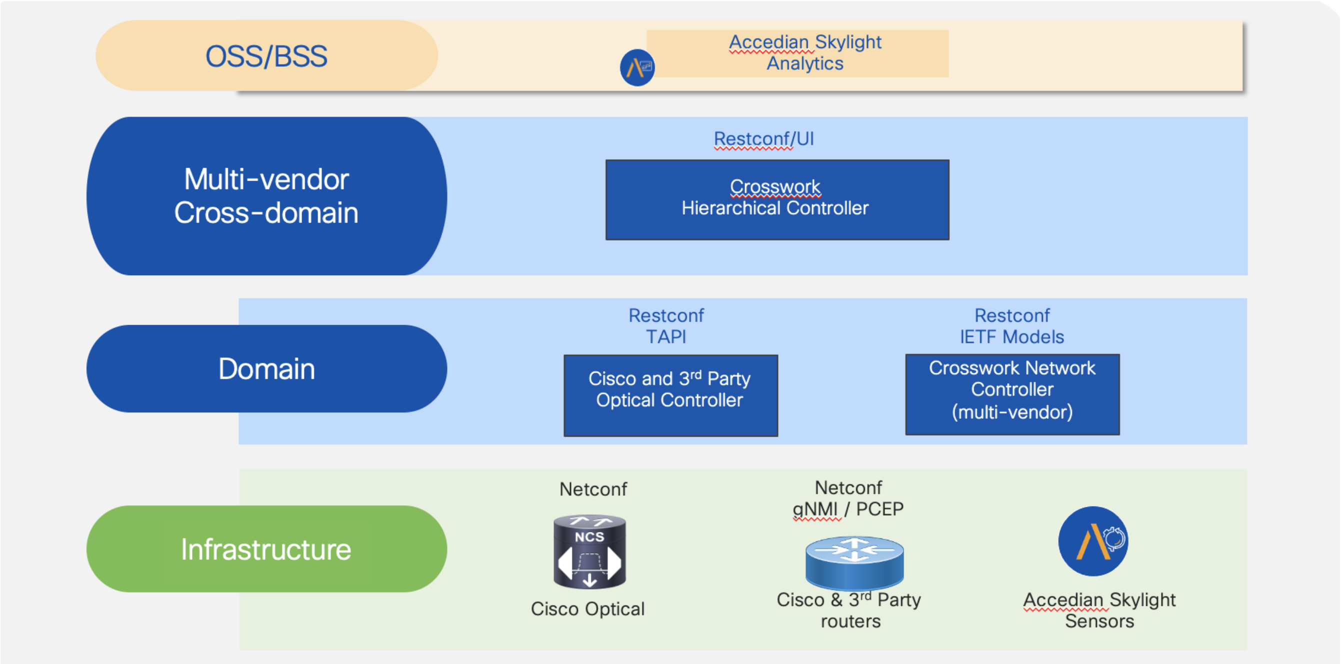
## Accedian Skylight Enhances Automated Assurance

Accedian is a technology partner to Cisco. It provides active assurance solutions for mobile networks and enterprise-to-data center connectivity, among other sectors.

Accedian's primary solution is Skylight which is used for active and passive performance testing and monitoring in IP, Ethernet, Mobile, SD-WAN, and cloud infrastructures.

Figure 4 shows Crosswork's alignment to Transport SDN Architecture with reference to Accedian Skylight. Accedian Skylight Analytics can be integrated with OSS tools to perform testing and assurance functions to complement service performance across SDN transport networks.

**Figure 4 Cisco Crosswork Alignment with IETF SDN Architecture**


OSS/BSS
Accedian Skylight Analytics
Multi-vendor Cross-domain
Restconf/UI
Crosswork Hierarchical Controller
Domain
Restconf TAPI
Cisco and 3rd Party Optical Controller
Restconf IETF Models
Crosswork Network Controller (multi-vendor)
Infrastructure
Netconf
NCS
Cisco Optical
Netconf gNMI / PCEP
Cisco & 3rd Party routers
Accedian Skylight Sensors

*Source: Cisco*

Active assurance provides a powerful technique for understanding the status and performance of the network. It simulates a network flow using active agents across one or many link paths measuring such things as latency, delay, jitter, and throughput for a given network or service flow. It also combines the end-to-end view with the health status of the transport and infrastructure layers that support the service. This provides the performance metrics necessary to confirm a consistent service level and to provide a high degree of confidence in 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.

Accedian Skylight provides service activation testing, network fault isolation, bandwidth monitoring, and service performance visibility from the user edge, core, and to the cloud to enable end-to-end service assurance. Skylight provides an end-to-end service view of the network at a granular microsecond level, and the solution is built on a time series database, analytics, workflow, and diagnostics. Because Skylight acts on real-time data, once established patterns and incident markers are identified, triggers can be activated within sub-seconds to take immediate action or continue monitoring while looking at additional parameters. Over time, a historical model of network and service performance is established, which can then be used to drive predictive analytics to further increase the insight provided to the users of the UI and to Crosswork by way of events and pre-processed and pre-analysed metric information.

Accedian partners with Cisco, augmenting the latter's multi-domain and multivendor controllers with the ability to validate SLAs and identify/isolate service delivery problems.

## Use Case – 5G Transport Network Slicing

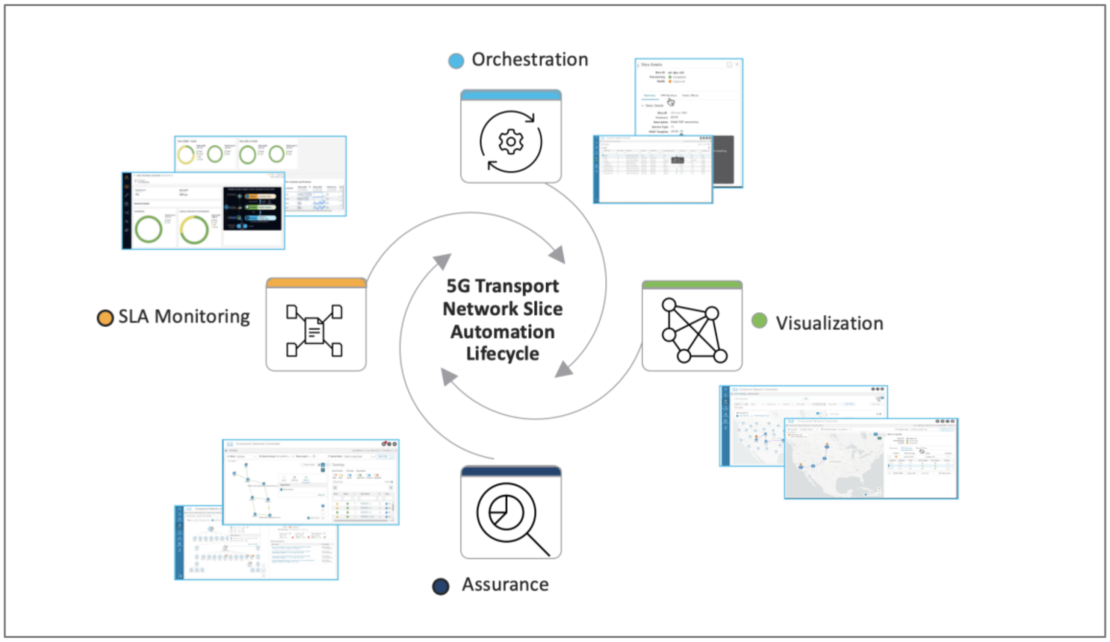
Cisco works closely with key customers to bring automated assurance beyond the lab and into live production. Network slicing is a good example of what intent-based automated assurance looks like: slicing guarantees that a selected service will be delivered through the network while meeting intended quality and service levels. Effectively, it dynamically partitions network resources and functions across multiple layers to deliver a unique service instance with defined quality metrics.

The Crosswork automated assurance use case for 5G network slicing  has been designed for 3GPP-defined 5G slices, starting with eMBB and URLLC. **eMBB** (Enhanced Mobile Broadband) defines the highest performance slice for 5G bandwidth, tripling download speeds for bandwidth-intensive applications, including AR/VR/XR.  **URLLC** (Ultra Reliability and Low Latency) defines the most latency-sensitive slice for 5G applications, including autonomous driving, remote surgery, and factory automation. A third slice, **mMTC** (massive Machine Type Communication), defines a further slice focused on IoT and robotics, dramatically expanding the number of connected terminals for a given slice and enabling Industry 4.0 use cases. Cisco intends to address this as the market matures.

Figure 5 depicts the automation lifecycle phases of transport network slicing.

Intent-based network slicing is a technique that enables the creation of logical networks that are optimized for specific services or applications. It involves creating network slices with specific characteristics such as bandwidth, latency, and reliability, based on the intent of the service or application. The life cycle of intent-based network slicing typically involves several stages, including resource allocation, domain level orchestration, test validation, and active assurance.

**Figure 5 5G Transport Slicing Automation Lifecycle**



*Source: Cisco*

Automated network assurance and SLA (Service Level Agreement) monitoring are key components of intent-based network slicing. Automated network assurance involves the use of AI and machine learning to automate network monitoring and troubleshooting, enabling network administrators to quickly detect and resolve network issues. SLA monitoring involves tracking network performance against predefined service level agreements, ensuring that the network meets the required levels of performance and availability.

With the network slices configured, the automated network assurance tools can monitor the network slices and quickly detect and resolve any issues that arise. This includes identifying issues with network connectivity, delay, jitter, and latency.

The SLA is continuously measured against the predefined SLAs, providing network administrators with real-time feedback on how well the network is meeting its intended goals. Any SLA violations are quickly identified and addressed.

By combining intent-based network slicing with automated network assurance and SLA monitoring, network administrators can create highly optimized networks that meet the specific needs of their applications and services, while also ensuring that the network meets the required levels of performance and availability.

A critical component to offering effective slicing is an earlier comment about needing a multi-domain, multi-layer platform to achieve an end-to-end intent-driven network, which also includes robust service assurance.  Cisco has worked internally and with partners and made strategic acquisitions to ensure they have checked all the boxes for CSPs interested in offering 5G slice technology.

## Conclusion

CSPs have invested hundreds of billions in network assets over the past decade, including high-speed fiber optic networks, IP overlays using software-defined networking, and containerization of network functions to deliver services at scale economically. This is the second technology wave to follow cloud-orchestrated infrastructure, where we see the opportunity zone for CSPs and the broader supplier ecosystem.

It promises to be as large if not more extensive than the cloud-orchestrated infrastructure wave. It promises to fuse together fixed, mobile, and satellite communications in a telco platform that promises to open new markets. This will be driven by Industry 4.0 initiatives and longer-term Web 3 which is a much more disaggregated network supporting blockchain and token-based economies.

Intent means that you match the business goals with what the network must be able to deliver. Let us assume that your internal business objective is to find the lowest cost link that satisfies an SLA required by the customer. Intent presumes that you define a service with specific business objectives that can then be translated to KPIs that can be supported by available resources in the network where the network is dynamically scaling in and out. Intent is fundamental to simplifying automation and reducing the future maintenance burden.

Our focus on assurance is a deeply held belief that you can’t automate what you can’t measure, and you can’t measure what you can’t see or observe. Automated assurance is not an independent system. It is a collection of key technology assets that allows operators to process massive streams of telemetry data in near real time and extract a signal from the noise. This requires applied knowledge of the different technology domains and a full view up and down the 7 layers of the protocol stack.

Executing intent-based networking requires CSPs to address traditional cultural, process, and system assumptions to reframe their network needs. Systems, including orchestration, observability, and assurance are maturing and are ready to initiate a second wave of technological innovation. The automated assurance market and the commercial software going into production today will allow CSPs to lean forward and begin their journey toward intent-based networking.

To meet critical success factors, we recommend that CSPs define what success looks like in the planning phase. Keep the scope of the problem small with a focus on two or three business objectives. Work with key suppliers to solicit input and solutions. Establishing some guidelines and a proof of business value is necessary to maintain momentum and justify incremental investments.

For more on our research on network automation, machine learning, edge, and private networks, see Appledore Research (www.appledoreresearch.com)

**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