Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
WHITE PAPER

Transform Your Transport Network for 5G-Advanced & Beyond

A Heavy Reading white paper produced for Cisco Systems

AUTHOR: STERLING PERRIN, SENIOR PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

5G service provider networks are evolving to incorporate wireline and wireless convergence, telco edge, open/virtual RAN (O-RAN/vRAN), multi-access edge computing (MEC), network slicing, and other innovations. At the same time, cloud providers are propelling advancements across the entirety of the service provider ecosystem. The industry is also experiencing a global increase in partnerships between communications service providers (CSPs) and hyperscalers, including the hosting of network workloads within the public cloud.

Transport has a vital role to play, but the nature of the CSP transport network is changing rapidly. Historically, transport has consisted of data communication appliances interconnected with dedicated circuits. Today, transport is evolving to a logical construct that rides atop any available hardware and connectivity service. Compute hardware that hyperscalers own and operate, along with the connectivity that hyperscalers use to interconnect compute hardware, become resources for CSPs to increase the reach of their transport network. They also enable CSPs to access enterprise customers that have a presence on the hyperscaler network. The key to success is a network operating system that effectively abstracts the mix of appliances, dedicated circuits, and underlay networks into a single, cohesive, feature-rich transport network.

This white paper makes the case for a "5G cloud-ready transport network" that is prepared for 5G-Advanced (and beyond) and can support public and private cloud across wireless and wireline access domains. It also provides a case study of one pioneering operator—DISH Wireless—that has built this type of transport architecture.

NETWORK TRANSFORMATION

Mobile operator strategic priorities

Having spent tens of billions of dollars on 5G spectrum and billions more on the radio access network (RAN) infrastructure to support 5G, the focus for network operators is now firmly set on monetization—for both consumer and enterprise services. Heavy Reading segments the monetization strategy into three pillars, as described below.

On the consumer side, the **first pillar is fixed wireless access (FWA)**, and it has emerged as the first big 5G use case serving as an alternative to legacy broadband technologies, primarily in underserved areas that have been uncompetitive. In 2022, for example, FWA captured 90% of net broadband additions in the US, supplanting cable and DSL. T-Mobile reported 124 million locations covered by FWA as of 2Q23, and Verizon reported 30 million FWA locations.

On the business side, the **second pillar is private wireless networks**. These networks have proven to be a primary early focus for mobile network operators with strong growth opportunities as new capabilities to be introduced in 5G-Advanced (and beyond) become available. Through 1H23, Omdia counted over 1,500 private LTE and 5G announcements, including a mix of trials, partnerships, wins, and commercial network rollouts. Private 5G was a leading technology for 56% of all newly announced deployments. Key verticals were manufacturing, transport and logistics, and energy and mining.

5G network slicing, a concept introduced by the 3GPP, will aid the deployment of private 5G, as well as other unique and differentiated 5G services. Network slicing enables the multiplexing of virtualized and independent logical networks on the same physical network infrastructure. Each network slice is an isolated end-to-end network tailored to fulfill diverse service requirements requested by a particular application. (Transport network slicing is covered in detail later in this paper.)

Industry partnerships are the third pillar in mobile network operators' (MNOs') network monetization strategies, with hyperscaler partnerships high on the list. Heavy Reading survey data shows that the top CSP drivers for partnering with hyperscalers are as follows:

- Ease of deployment
- Accelerated service time to market
- Enhanced cloud-based security

This paper describes hyperscaler partnerships in detail in the next section.

Most recently, interest in CSPs partnering with satellite operators has risen sharply, driven by a need for expanded mobile coverage and the advent of standardized connectivity between satellites, smartphones, and other types of devices that are just starting with 3GPP Release 17. For mobile and fixed operators, satellite is an opportunity to rapidly expand coverage to remote locations and connect devices and customers worldwide. For satellite operators, collaboration with telcos can bring millions of new customers and devices to their systems.

Mobile operator network priorities

On the network side, operators are prioritizing the technical work that needs to be done to monetize the 5G networks that have been built over the past five years. They are also increasing the efficiency of their networks and reducing total cost of ownership (TCO) as network traffic and subscribers continue to increase. The network priorities described below are interrelated and are happening concurrently:

- **Migrate from non-standalone (NSA) to standalone (SA) mobile core:** Initial 5G launches supporting enhanced mobile broadband (eMBB) use cases were based on existing LTE mobile cores. However, 5G SA cores are required to launch many capabilities supporting ultra-reliable low latency communications (URLLC), massive machine-type communications (mMTC), and network slicing use cases. As of 2Q23, 116 operators globally were investing in public 5G SA networks, according to the Global mobile Suppliers Association (GSA). 5G SA cores are based on cloud native architectures.
- **Prepare for 5G-Advanced:** While SA cores are required to support 5G's unique capabilities, those capabilities still need to be standardized and commercialized. Operators are preparing for the set of features that will come with 3GPP Release 18 (also known as 5G-Advanced), which is slated to be completed in 1Q24. 5G-Advanced features will include support for non-terrestrial networks (NTN), among many other new capabilities.

- **Adopt RAN decomposition and virtualization:** RAN decomposition breaks the RAN down into individual components, including radio unit (RU), distributed unit (DU), and central unit (CU). Virtualization allows the DU and CU functions to run on commercial off-the-shelf (COTS) hardware, eliminating specialized hardware. Benefits include better utilization, greater scalability and flexibility, and cost reductions. Implementing decomposition and virtualization using O-RAN promises these benefits while also breaking RAN vendor lock-in due to standardized, open interfaces. Significantly, RAN virtualization was the number one network priority cited in Heavy Reading's 2023 *5G Transport Global Survey*—marking the first time that virtualization has reached the top spot.
- **Build out edge infrastructure:** Edge computing brings processing closer to the end customers and is essential for many of the emerging enterprise use cases, along with 5G SA and 5G-Advanced. Low latency, for example, is ultimately dependent on the physical distance between the customer and the network processing. Edge compute is also a top driver for cloud native adoption.

SERVICE PROVIDER AND HYPERSCALER PARTNERSHIPS

Why are they partnering?

Operators are migrating to cloud architectures—both public and private—to accelerate services and innovation, increase network flexibility and scale, improve efficiencies, reduce vendor lock-in, and reduce capex and opex costs. Cost savings from the cloud come by way of increased efficiency, reduced hardware costs, greater scalability and agility, and reduced staff and maintenance costs. Specific benefits sought by operators will vary by the domain in which cloud technology is applied, such as in IT operations, operations and business support systems (OSS/BSS), or telco workloads.

However, network operators have also learned first-hand that building a cloud requires specialized skills, and many have tried and failed on their own. To succeed, operators are turning to partnerships with hyperscalers. They recognize that hyperscalers have the necessary scale, technology, and expertise, and these advantages increasingly outweigh the risks of competitive conditions that may arise (e.g., competition for enterprise customers).

While cost savings is an important driver for moving to cloud architectures in general, it is not a primary motivation for why CSPs seek to partner with hyperscalers. Rather, ease of deployment is the most important reason for partnering with hyperscalers by far (based on Heavy Reading survey data), followed by accelerating service time to market and enhancing cloud-based security. The top two drivers—ease of deployment and time to market—are even more important for the largest operators, Heavy Reading finds.

CSP workload and network requirements

Partnerships between CSPs and hyperscalers cover an array of models, including the following:

- CSP connectivity services sold through cloud provider marketplaces (e.g., Rakuten)
- CSP resale of cloud services (such as Microsoft 365 and Teams)
- Bundled services/go-to-market initiatives
- Co-development

Hosting workloads in the public cloud is also gaining momentum, with most operators (to date) moving their IT OSS/BSS to the public cloud.

Hosting network functions in the public cloud is less common and more controversial, however, as the network represents the "crown jewels" of a network operator. CSPs have very different workload requirements compared to most enterprises that cloud providers have historically served. CSP performance requirements include high throughput, strict latency and jitter budgets, high reliability and redundancy, and on-demand scaling. Government regulation drives other requirements, such as service continuity mandates, data sovereignty, and security. From a network perspective, dynamic routing and routing features at scale, network separation, traffic isolation, geo-redundancy, link and network error detection, and standard routing technologies (no cloud lock-in) are required in the public cloud.

While some operators consider network functions out of scope for public cloud on principle alone, others are moving forward with this model. Some—most notably AT&T and DISH Wireless—are moving aggressively.

Figure 1 shows a sample of high profile CSP/hyperscaler partnerships specifically involving network workloads, with statuses ranging from test and proof-of-concept (PoC) to commercial deployments.

Figure 1: Notable CSP and hyperscaler cloud partnerships for network workloads

CSP	Hyperscaler partner	Description	Date announced
Orange	Amazon Web Services (AWS)	End-to-end, cloud native 5G SA experimental public and private cloud network named Pikeo.	February 2023
Swisscom	AWS	PoC trial with 5G core applications running on AWS, with more applications to be added successively as the project progresses.	March 2023
O2 Telefónica	Google Cloud	5G cloud core network to deploy and test customer applications and networking for mobile broadband, network slicing, real-time applications, and private 5G networks.	December 2022
DISH Wireless	AWS	World's first CSP to deploy cloud native, 5G SA core on a hyperscaler cloud.	February 2022
AT&T	Microsoft Azure	Strategic alliance through which Azure acquired AT&T's Network Cloud platform technology and AT&T moved its 5G core network to the Microsoft cloud.	June 2021

Source: Heavy Reading

Why hybrid cloud for service providers?

As detailed above, operators see tremendous value in cloud architectures generally and in public cloud specifically for some—but not all—use cases, functions, and workloads. Thus, operators will use their own private cloud in certain cases and public cloud in others. Some operators will pursue public cloud-hosted network functions aggressively, while others will approach public cloud network functions more cautiously, and still others will wait and see how the market evolves.

Factors weighed in public versus private cloud decisions include privacy, security, latency, speed of deployment, internal comfort levels, and others. **Figure 2** compares the advantages and common functions for on-premises and public-hosted deployments.

Figure 2: On-premises vs. public-hosted network functions

	On-premises	Public
Advantages	Required for physical devices (RU, GNSS, antenna)	Ease/speed of deployment
	Proven architecture, widely adopted by service providers	Ability to scale horizontally within minutes
	Ultra-low latency to meet O-RAN requirements (O-DU latency requirements)	Flexible compute capacity offering
	Proximity to most endpoints	Wide array of services (e.g., Internet, Load Balancer, Kafka, etc.)
Typical functions	RU	5G packet core, IMS, voice, and data plane UPF
	DU	CU, RAN management, and radio intelligent controller (RIC)
	DNS, DHCP, and IP address management	Observability, automation, and orchestration

Source: Cisco, DISH Wireless, Heavy Reading

This means that, for the foreseeable future, hybrid cloud will play a dominant role in the communications industry. The hybrid cloud architecture will include a mix of private clouds, centralized public clouds, and on-premises public cloud deployments.

5G TRANSPORT NETWORK EVOLUTION

The converged, cloud-ready transport network is required to address all the requirements described in the previous section. The four key transport network components are as follows:

- Converged infrastructure
- Programmable transport and network slicing services
- Cloud-ready infrastructure
- Simplified operations model

Heavy Reading discusses each of these four components below.

Converged infrastructure

This white paper has focused primarily on the 5G network evolution, but most network operators offer services to a mix of customer types, including consumers, businesses, and wholesale customers. They support those customers with both wireline and wireless access network infrastructure. Further, "wireline" and "wireless" are themselves broad categories. Wireline can include DSL, cable, and PON for residential services and Ethernet and wavelength networks for enterprises. Wireless access encompasses primarily 4G and 5G-based services for mobility and (as noted earlier) FWA as a growing opportunity for MNOs in broadband. Most recently, standardized direct satellite-to-device connectivity is being defined in 3GPP NTN, starting with Release 17.

A truly converged transport network is built to handle most—and ideally all—types of access services and technologies on a single network infrastructure with a combination of IP routing and optical/DWDM. IP and optical can be physically converged with IP over DWDM (a.k.a. routed optical networking).

Programmable transport and network slicing services

At the packet layers, Border Gateway Protocol (BGP)-based VPNs and segment routing (SR) are two essential technologies for converged, packet-switched 5G transport. In this architecture, BGP-based VPNs make up the overlay services layer, while segment routing based on either MPLS or SRv6 forms a unified underlay packet-switched network.

The services layer provides connectivity details to all mobile and fixed IP services in the converged network. Meanwhile, the underlay infrastructure provides basic network services, such as per-hop-behavior quality of service (QoS), fast route convergence, SR traffic engineered-based forwarding for intent-based path selection (shortest path, lowest delay, disjoint, etc.), scaling, and timing.

Although setting up all these functions individually allows the operator to provide granular customization for clients or services, this level of service design creates some complexity in other areas. It drives very long development timelines, service rigidity, and northbound OSS/BSS layer integration work. In addition, it is not as flexible as desired by cloud-like users who want declarative services and "on-demand" simplicity.

Network slicing for 5G and beyond

Network slicing defines expected outcomes, or intent, which drives simplification of the requested service. The idea is that providing a flexible, outcome-based, on-demand experience for users will drive new use cases and, thus, revenue streams for the provider.

Virtualization and logical networking are not necessarily new in transport. As discussed above, there are well-defined Internet Engineering Task Force (IETF) technologies that, working together, can provide "logical" based service guarantees over a single physical network. What is new for transport is using the intent-based slicing concept. With intent-based slicing, network operators can abstract the complexity of service provisioning (via a controller)—whether for 5G use cases or others—into simple service-level objectives and expectations.

Slice virtualization is a new concept for the radio and 5G core domains, which (with the transport domain) make up the end-to-end mobility slice service components as defined by 3GPP. All three sub-domains must be orchestrated "in concert" for the end-to-end slice service to be successfully deployed by a top-level 3GPP-defined network slice management function (NSMF) controller. While 3GPP is addressing the specifications for most of these components, it has not focused on the transport domain.

That should be acceptable, as the IETF is the primary standards body responsible for packet transport, including the IP VPN, BGP, MPLS, IPv6, QoS, and SR technologies referenced above. Thus, the IETF has taken the lead in defining the specifications for what it calls an "IETF Network Slice,"* which is specific to only the transport domain requirements. It also defines an IETF Network Slice Controller (NSC), which is the automation element that abstracts the transport network complexity into simple intent-based slicing service requests that can be presented northbound via a well-defined slice YANG model.** In theory, this YANG model can provide a transport slicing API interface that can be used by the top-level 3GPP end-to-end slice controller (NSMF) for stitching end-to-end slice services across all domains.

5G network slicing has taken off more slowly and cautiously than many predicted. Early implementations are mostly capacity-based slices, such as dedicated slices for delivering enterprise FWA. These are preconfigured eMBB slices that are limited and static. However, with the adoption of 5G-Advanced, 5G SA cores, and edge expansion, Heavy Reading expects to see the adoption of service-specific network slices in 5G, including eMBB, URLLC, and mMTC use cases, deployed on a shared network.

Significantly, transport providers can also develop their own types of transport slices beyond the 3GPP-defined ones. Examples include "encrypted slices" (where traffic only transits encrypted link types using MacSec), disjoint path slices (where there are no common links or nodes across these slices), regional avoidance slices, and high-speed link slices, among others. These transport slice services will be available for all transport customers, not just 5G, and will allow providers to differentiate from each other and drive a more cloud-like user experience.

** https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-25*

*** https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-08*

Cloud-ready infrastructure

As noted, there is no "one-size-fits-all" approach to cloud workload adoption. Each operator will have its own strategy and timeline, with options including public, private, on-premises public, and hybrid combinations of public and private cloud. Furthermore, as operators progress along their timelines, the composition of workloads across public and private deployments will change. (Heavy Reading survey data shows that operators expect the share of public cloud workloads to increase over time.)

The underlying transport network must be agnostic as to whether the workloads are public or private or whether the workloads are on-premises or colocated. Virtual routers play an important role in providing required IP networking functions (e.g., BGP-VPN, SR, QoS) in public and private cloud environments.

These virtual routers, however, must deliver the same levels of functionality, scale, and performance as the physical routers they replace. Ideally, they also provide the same management look and feel as the physical routers deployed in the network.

The key point is that it all looks like one network to the network operator regardless of workload type and location.

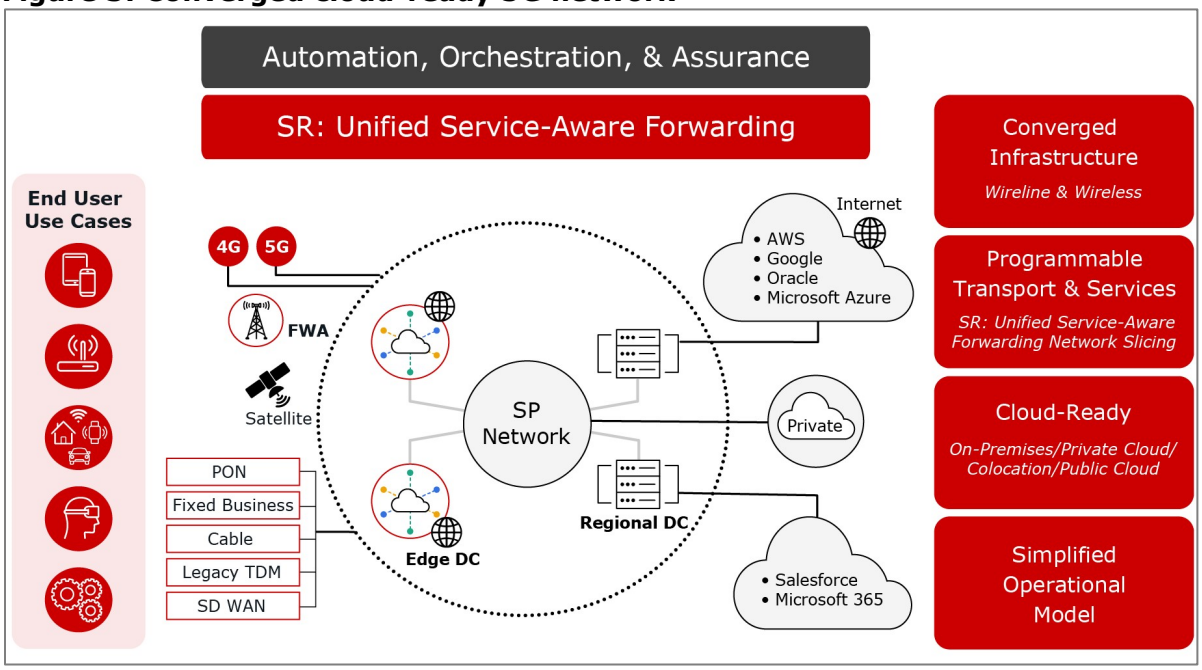
Simplified operations model

Lastly, operators require a simplified network operations model with service assurance as they move to next-generation architectures. Network automation is an important tool for operational simplification and driving opex reductions.

Network modernization initiatives provide an ideal insertion point to introduce automated network functions into the network at scale. Operators require new transport networking equipment to have extensive telemetry and open APIs that allow easy access and programmability from northbound orchestration and/or controllers.

Figure 3 illustrates a converged cloud-ready 5G transport network with multiple access domains and a hybrid cloud.

Figure 3: Converged cloud-ready 5G network



Source: Cisco, Heavy Reading

DISH WIRELESS CASE STUDY

DISH Wireless is the fourth largest wireless carrier in the US by subscribers. It has been an enthusiastic early champion of O-RAN and the public cloud, believing that these new architectures will enable it to bring new services to market faster and more cost-effectively than relying on single-stack vendor systems and traditional deployment models.

In June 2023, the operator met its US government obligations to cover 70% of the US population with 5G—amounting to 240 million people covered. Additionally, as a greenfield build network operator, DISH Wireless has built a 5G network based entirely on a 5G SA core. The SA core makes the operator well-positioned to offer services based on 5G-Advanced functions as they become available.

DISH Wireless xHaul transport architecture

The DISH Wireless architecture consists of both on-premises and public cloud hosting of network functions. The public cloud network design uses a logical hierarchal architecture consisting of national data centers, regional data centers, and breakout edge data centers, which are in cloud provider local zones across the US footprint.

Additionally, DISH Wireless hosts network functions in on-premises locations that are not part of public cloud. On-premises locations include a mix of distributed RAN (D-RAN), local data centers aggregating centralized RAN (C-RAN) cell sites, and passthrough edge data centers that aggregate traffic from all LDCs and cell sites in each market and hand off to the public cloud.

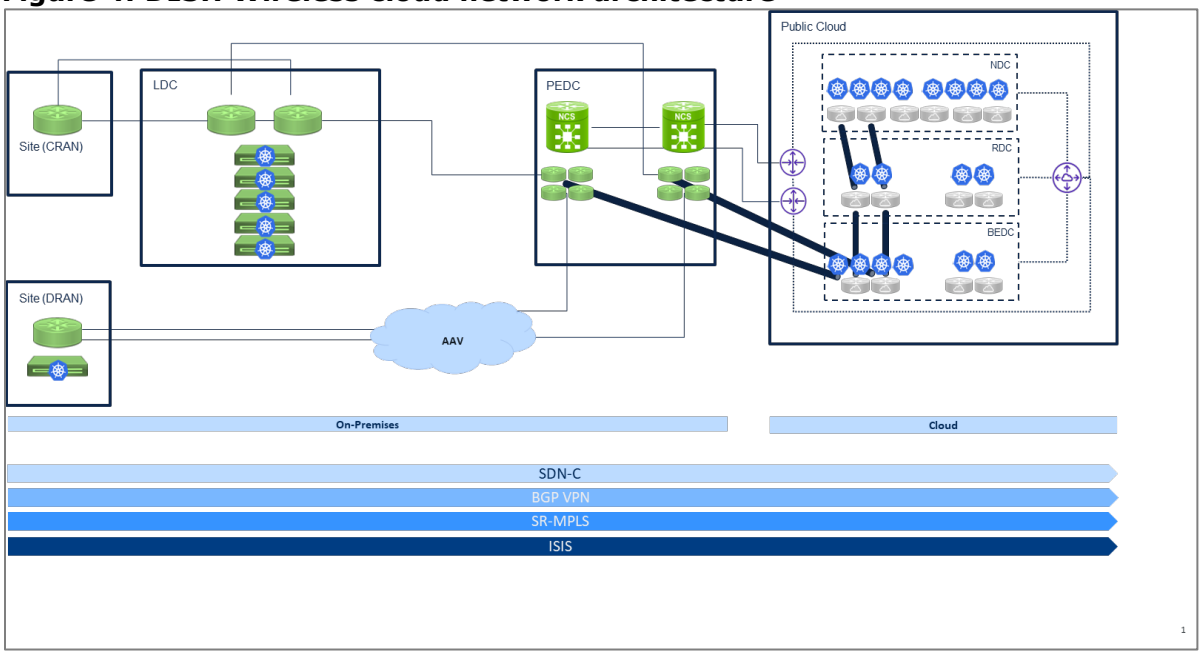
DISH Wireless connectivity is based on a unified routing domain using industry-standard routing technologies to enable connectivity that is agnostic to where the workload is located—whether on-premises or on cloud. The operator intends to move to multicloud over time. For this reason, it was important to remove any cloud-specific dependencies and/or obstacles while also simplifying the engineering and operations of the network with the same look and feel.

Segment routing-MPLS (SR-MPLS) with BGP-VPN has been deployed across on-premises and public cloud in the DISH Wireless network. A centralized software-defined networking (SDN) controller orchestrates, automates, and provides unified service enablement in a hybrid cloud/multicloud environment with end-to-end network visibility.

Cisco is DISH Wireless' supplier for packet transport, automation, and the complete lifecycle of advanced services for the transport domain. Specific products include Cisco's NCS540 for cell site routing, ASR9K and NCS5700/NCS5500 for edge and aggregation functions, Nexus 9000 for data centers, and Cisco XRv9K for virtual routing in the cloud. For automation, DISH Wireless relies on the Cisco Crosswork Network Controller.

Figure 4 depicts the DISH Wireless network architecture.

Figure 4: DISH Wireless cloud network architecture



Source: DISH Wireless

Hybrid cloud deployment challenges and learnings

As a pioneer in public cloud architecture, it is no surprise that DISH Wireless had challenges in its network and service rollout. In routing, DISH Wireless found limited dynamic routing and scalability in the cloud. In the public cloud, the operator found that latency is difficult to predict. And in terms of throughput, DISH Wireless encountered per-flow traffic limits at the interface level and packet-per-second limits based on the type of instance.

These challenges required architectural changes and thorough testing to overcome. The resulting architectural changes are reflected in the DISH Wireless architecture described in the case study. Joint developments among DISH Wireless, Cisco, and the public cloud operator were essential. One key to success was establishing a detailed baseline, service delivery, and validation framework for service provider network functions, as well as a baseline performance for instances.

Another key was building a unified overlay service provider network across on-premises and public cloud to supplement cloud routing. Requirements here included virtual routers with the same look and feel as physical routers in the public cloud. The routers enabled unified forwarding in the hybrid cloud (and ultimately multicloud) with QoS, the ability to scale routes independently from the cloud network, and unified end-to-end visibility with service assurance.

CONCLUSION

Network operators are entering a new phase of evolution and opportunities based on a combination of a 5G SA core, 5G-Advanced, MEC, and RAN virtualization. In a challenging environment, operators must focus on monetization while also running networks as efficiently and flexibly as possible.

To meet their goals, operators increasingly see tremendous value in cloud architectures generally and in public cloud specifically for some use cases, functions, and workloads. Private cloud, public-hosted, public on-premises, and traditional functions must coexist in hybrid architectures.

A 5G cloud-ready transport architecture will support 5G-Advanced and beyond, including fixed and mobile wireless and wireline services. Heavy Reading identifies four key components of a converged transport network, as follows:

- Converged infrastructure
- Programmable transport and network slicing services
- Cloud-ready infrastructure
- Simplified operations model

While it is early, a 5G transport blueprint is beginning to emerge, as evidenced by DISH Wireless' pioneering hybrid cloud architecture supporting 5G.