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

HEAVY READING
WHITE PAPER

Simplifying Operations with Multi-Layer Network Control

A Heavy Reading white paper produced for Ciena

AUTHOR: JENNIFER CLARK, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION: CATCHING UP WITH CHANGE

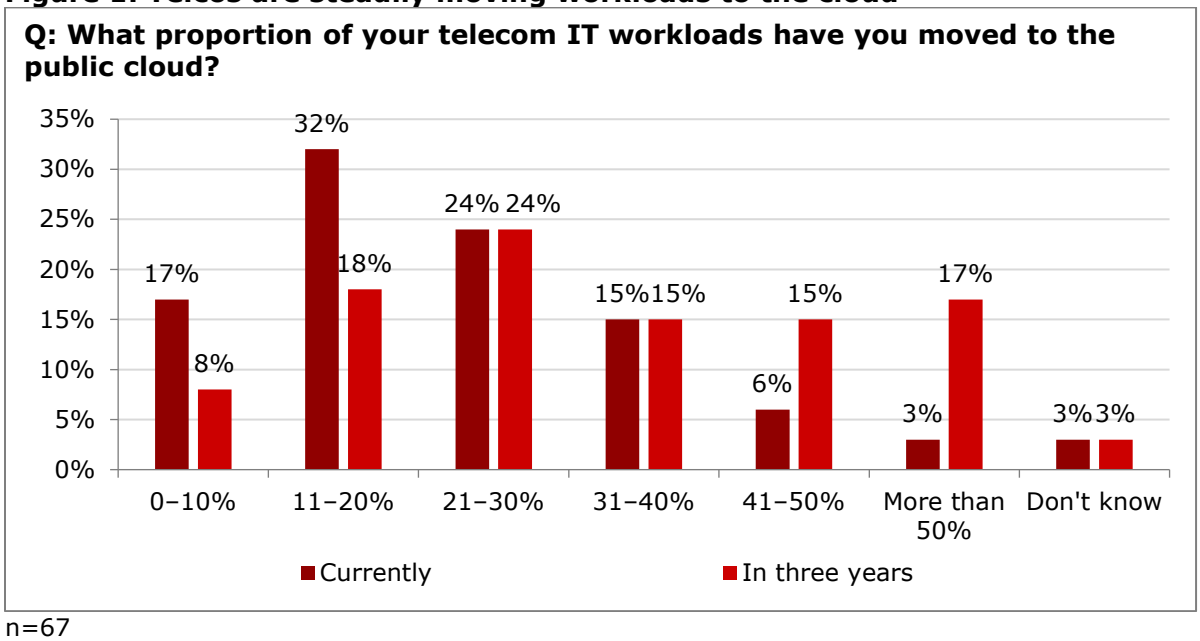
The expansion of the network is as inevitable as the expansion of the universe. Heavy Reading calculates that 2.5 quintillion (that is 25 followed by 17 zeros) bytes of data are generated *daily*. The growth rate of this figure is constantly accelerating due to the increase in the number of devices (e.g., Internet of Things [IoT]), the evolution in data formats (e.g., 4K and 8K video), and the move to 5G. New applications such as the connected car and ultimately the fully autonomous vehicle (one AV will generate about 4 terabytes of data each day, Intel estimates) will also contribute to the huge proliferation of data.

CSPs, along with enterprises, are moving workloads to the cloud

Data expansion is not confined within the borders of the enterprise. Heavy Reading research shows that 45% of enterprise workloads are now run in some form of cloud computing, an increase from 35% in 2020 and 25% in 2019. The COVID-19 pandemic has not slowed cloud migration. In fact, according to Heavy Reading's research, the pandemic has accelerated it.

The migration of workloads to the cloud applies to the telcos, as well (see **Figure 1**). Communications service providers (CSPs) are looking to extend their reach into new services or verticals (e.g., telco networks, financial services, Industry 4.0, healthcare) and markets (e.g., new geographies) in a cost-effective way. Partnering with the hyperscalers also allows the CSPs to develop their technology and service capabilities (e.g., cloud, software, multi-access edge computing [MEC] for telcos).

Figure 1: Telcos are steadily moving workloads to the cloud



n=67

Source: Heavy Reading, Omdia, Service Provider Digital Transformation and Cloud Strategy Survey – 2022

The shift of telecom IT workloads to the public cloud is steady. Over half of CSPs have already moved between 10% and 30% of their workloads to the cloud. Only 9% have moved a substantial 40% or more of workloads. However, in three years, this percentage is expected to more than triple, with a third of all carriers moving 40% or more of their workloads to the cloud. Nevertheless, trailblazers such as AT&T—which has publicly announced that it will migrate most non-network workloads to the public cloud by 2024—remain the exception.

The law of big numbers and perpetual network expansion

Understanding the network is like going to a planetarium show, where the numbers thrown around quickly cause your eyes to glaze over at the unfathomable vastness of space: 100 billion stars in the Milky Way galaxy, 125 billion galaxies in observable space, etc. Or, in the case of the network:

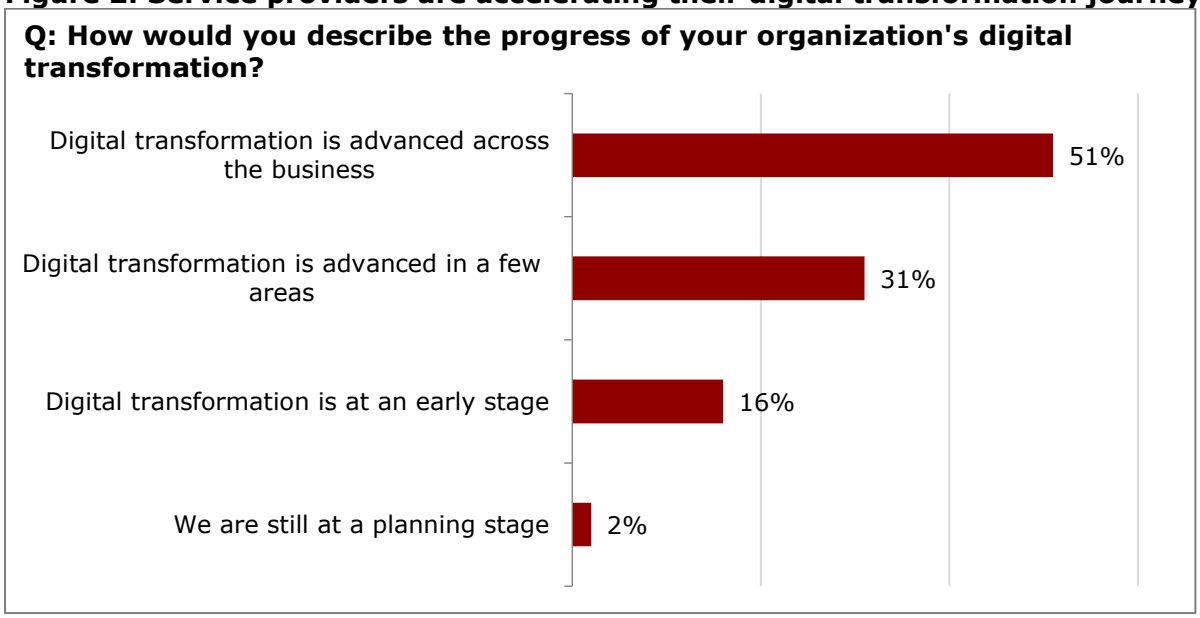
- **7.5 million cell sites** worldwide in 2022, with 5G and small cells expected to grow to 40 million in 2030.
- **Approaching 10 million optical coherent ports** in operation.
- **9.9 billion global installed base of connected devices** in 2022, growing to an estimated 11.29 billion devices in 2027. This figure includes PCs, tablets, laptops, smartphones, set-top boxes, smart TVs, game consoles, and more. It does not include IoT devices.
- **32.37 billion global installed base of IoT devices** in 2022, growing to an estimated 49.55 billion in 2026.

How do you measure this environment, let alone manage it? There is one word that will resonate with any CSP managing the network today and looking down the road at the expanding network that will need to be managed in 2027: simplify. In this report, Heavy Reading examines how CSPs can simplify network management through the *automation of multi-layer operations.*

CSPs are under pressure to recast themselves as digital service providers. To achieve this, they are pursuing digital transformation strategies. Heavy Reading defines digital transformation as the process of adopting and deploying new digital technologies that result in fundamental changes supporting new business models and enabling organizations to compete and work with other digital companies. It is a multidimensional transformational change that affects all aspects of the telecom service provider business, including customer interaction, operational processes, networks, technologies, architectures, organizational culture, and people. *Digital transformation is an ongoing journey, not an end state.*

Heavy Reading has been tracking the network transformation of the carriers. In our 2022 Carrier Survey, 82% of CSP respondents claim that digital transformation is "advanced" across all or some areas of the business, a similar percentage to last year. However, 51% claim it is now well advanced across the business, compared to only 39% last year, suggesting transformation is becoming less siloed and more pervasive.

Figure 2: Service providers are accelerating their digital transformation journey



n=67 global network operators
Source: Heavy Reading, Carrier Survey 2022

"SIMPLIFY, SIMPLIFY": DEALING WITH AN OBSOLETE NETWORK MODEL

"Our life is frittered away by detail. Simplify, simplify," opined Henry David Thoreau in his classic Walden. (To which pal Ralph Waldo Emerson quipped: "One 'Simplify' would have sufficed.") As networks, applications, and data expand, the information available to manage, analyze, and troubleshoot networks also expands exponentially. The industry has reached a point in the evolution of networking, however, where we have an opportunity to simplify the management of networks to the benefit of the CSP and the customer.

When discussing network management and operations with a network technician, it is rarely more than a few minutes before the OSI network model enters the conversation. The seven-layer model starts at Layer 1, the physical layer, and runs through Layer 7, the application layer. It is a useful way to visualize the tasks associated with a communications session. Each layer operates independently of the layer above and below, making a very diverse network possible—with the potential for dozens of protocols at each layer.

However, this is not a productive way to visualize the network in 2022. Today, there is functional standardization at each of the three lower layers:

- **Layer 1, physical layer – fiber:** With copper being actively phased out by both carriers and countries, cable, fiber, and wireless are being used as access technologies. The media used in the metro, core, and long-haul network media is ubiquitously fiber.
- **Layer 2, data link layer – Ethernet:** The function of Layer 2 is similar to that of Layer 3. The most significant difference is that Layer 2 facilitates the data transfer between two devices on the same network. It also breaks the packets received from the network layer into frames.
- **Layer 3, network layer – IP:** The internet protocol (IP) comprises 95% of all internet traffic.
- **Layer 4, transport layer – various:** Responsible for the logical communication between applications running on different hosts. While Layer 4 is dominated by TCP, there is still a fair amount of protocol diversity with UDP, ICMP, BGP, and more. Layer 4 functions as the dividing line between network infrastructure and network applications.

Converged IP/optical infrastructure

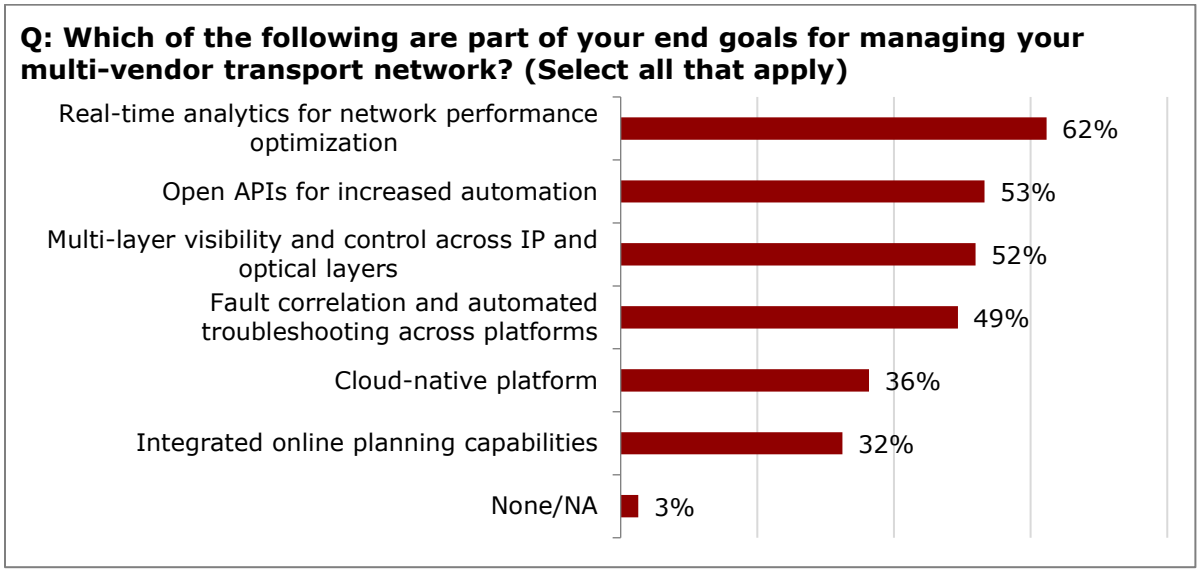
Cloud and 5G services will run over a converged IP/optical infrastructure. The question becomes: Why do we even refer to the OSI stack? From the late 1980s and into the 1990s, the industry experienced "the internet–OSI standards war." The IP suite (TCP/IP) won this dispute, which ultimately resulted in the die-off of most other protocols. Goodbye AppleTalk, Token Ring, StarLan, X.25, Frame Relay, ATM, SNA, DECnet, XNS, Banyan VINES, and Novell NetWare, to name only a few. Some of these protocols continue today, but in pockets and private networks.

Similarly, OSI Layers 1–3 were once plump with protocols, diversity, and complexity. Today—while still plenty complex—they are comparatively skinny layers that have been simplified by protocol attrition and streamlined by decades of industry-standard practices. Why are we managing them as separate layers? *The CSPs have a stellar opportunity to manage Layers 0 (the photonic or DWDM layer) through 3 as one unit—and take a giant step toward operations automation and digital transformation.*

OPERATIONS TRANSFORMATION IS NEEDED

CSPs need to simplify, accelerate, and automate network operations. To accomplish this, they are looking at an evolutionary upgrade in network management visibility and automation. With Layers 0 through 3 converging in network architectures, there is demand for merged Layer 0–3 visibility and control while acknowledging the fact that support for multiple technology layers requires support for multiple vendors. The CSPs exhibit a growing consensus regarding multi-layer management. They are looking for real-time analytics, open APIs, and multi-layer visibility to enable the management of their multi-vendor transport network, as seen in **Figure 3**.

Figure 3: CSPs' top management objectives for their multi-vendor transport network



n=77

Source: Heavy Reading, Transport Automation Survey 2022

Fragmented legacy network management system (NMS) tools make operational processes error-prone and time-consuming. Today, each functional layer of the network (optical, Ethernet, IP) uses its own NMS. Each vendor or device type can also employ its own element management system, and each virtual/containerized network function can have its own virtual/cloud native network function (VNF/CNF) manager. By leveraging software-defined networking (SDN) domain controllers, CSPs can move to a single pane of glass for infrastructure management. Domain-specific controllers provide the essential bridge between physical and virtual infrastructure elements and higher order multi-domain orchestration systems.

SDN domain controllers assume a pivotal role

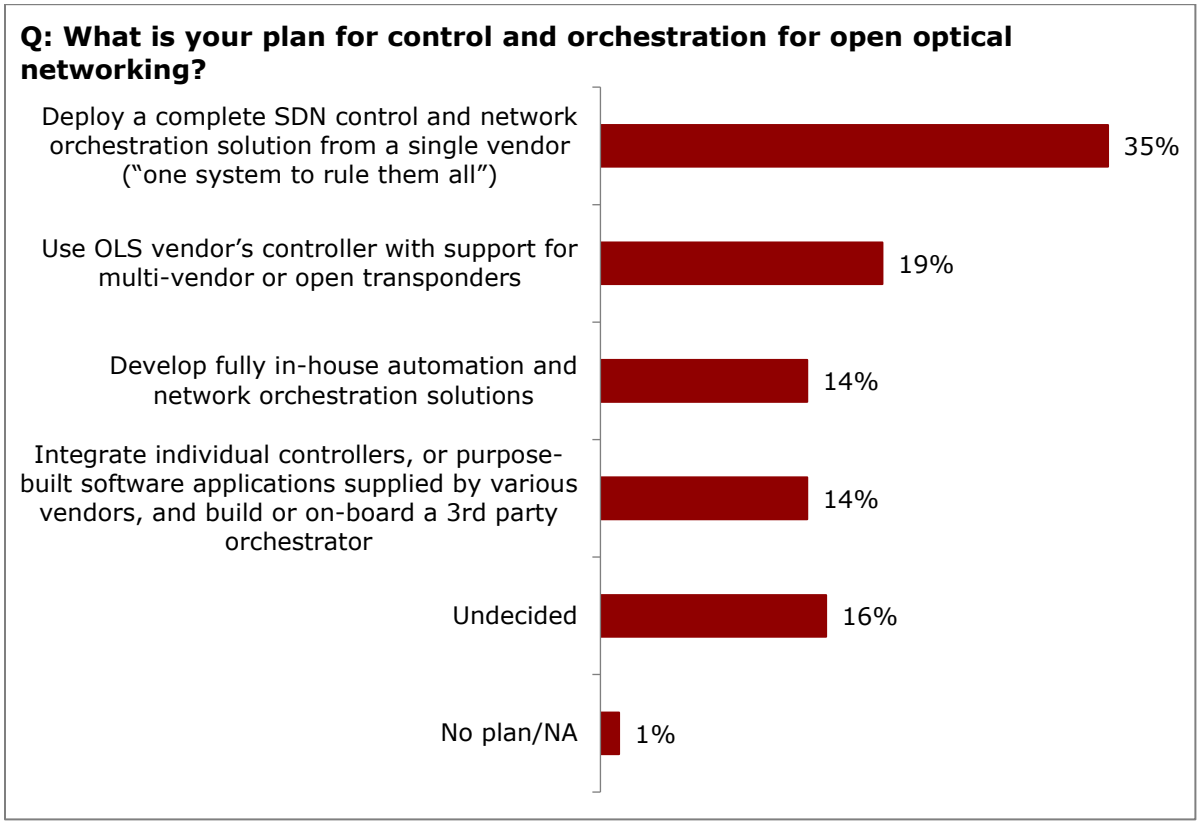
Most CSP networks today operate with network intelligence embedded in each distributed network device. SDN and its associated OpenFlow protocol emerged in 2008 with a goal of improving performance and lowering the cost and complexity of network routers by separating the control and data planes. The external, centralized control plane was responsible for all management and routing functions. All routing and forwarding

decisions were made by the control plane. This early vision of SDN did not really materialize within CSP networks, as it required the complete reconfiguration of the network. In addition, gaps existed, such as the lack of support for local protection and an inability to reroute quickly and automatically around failures.

However, SDN and SDN controllers have become crucial in managing and automating multi-layer, multi-vendor networks. SDN has provided a standard way to talk to devices and the ability to enhance network programmability through standard protocols and open interfaces. SDN controllers enhance network decision-making by centralizing and leveraging data that would not be practical to be used, from either a cost or performance perspective, across distributed network devices. Embedding complex functions into device-level software is difficult and costly and makes upgrading those devices similarly difficult, costly, and vulnerable to error, whether human or software generated.

With SDN controllers, CSPs can optimize both centralized and distributed network resources. They can provide a unified view across optical, Optical Transport Network (OTN), Ethernet, and IP infrastructure, speeding up problem detection, fault correlation, and root cause resolution. This view, in turn, enhances network visibility and drives business agility. CSPs appear ready to implement an SDN solution, ideally from a single vendor, as shown in **Figure 4**.

Figure 4: CSPs want one SDN control and network orchestration solution from one vendor



n=77

Source: Heavy Reading, Transport Automation Survey 2022

Moving to the zero-touch NOC – cloud native and cloud hosted

In March 2020, at the start of the COVID-19 pandemic, CSPs were confronted with an abrupt (virtually overnight), unplanned move to zero-touch network operations centers (NOCs) and lights-out data centers across many of their geographies. The pandemic illustrated, like an early warning system, the challenges that CSPs face with the unchecked expansion of cell sites, network nodes, network data centers, devices, and traffic. CSPs can no longer afford, in terms of either cost or performance, to manage their networks as static, manned data centers relying on operator intervention for problem resolution. The need for automation combined with artificial intelligence/machine learning (AI/ML) came into sharp focus, accelerating digital transformation within the CSPs.

Part of the lessons learned, or at least reinforced, included the need to create a more agile, scalable network by transitioning to a cloud native architecture. The move to cloud native, with its associated containers and microservices, facilitates the automation of all stages of the network lifecycle—design, implementation, and day-to-day operation. It enables greater flexibility relative to how to manage the network and where to place the SDN controllers: in the NOC, in the public cloud, or as a hosted solution by the SDN controller vendor.

PROVIDING THE GLUE: APIS

Standard and open APIs are central to network visibility and operations automation as implemented in SDN-controlled transport networks. Open APIs are used to communicate northbound to operational support systems (OSS) and southbound to network elements. They enable workflows that involve operational systems to be automated—including customer care, billing, inventory, and multi-vendor orchestration.

The industry is coalescing around a group of standards and APIs. Up until now, the many SDN standards have caused confusion among the CSPs, a drag on the SDN market, and roadblocks to transport network automation. Open APIs, such as NETCONF, RESTCONF, gNMI, gRPC, OpenConfig, and RESTful APIs, share network data in a non-proprietary manner, enabling them to be used in a multi-vendor, multi-layer (e.g., optical and IP) domain management:

- **NETCONF** is a protocol that is widely implemented. It is defined by the Internet Engineering Task Force (IETF) as used to "install, manipulate, and delete the configuration of network devices."
- **gRPC Network Management Interface (gNMI)** leverages the gRPC Remote Procedure Call (gRPC) framework for configuration management and streaming telemetry.
- **RESTCONF** has become the de facto standard for controller-to-controller interaction, both north- and south-bound.
- **OpenConfig** is an open source project used to define and implement a common, vendor-independent software layer for network device management.

Network monitoring, service monitoring, and traffic engineering data are sent northbound from all Layer 0–3 devices in the CSP's network, irrespective of the vendor, to the SDN controller. This process enables a comprehensive view of the current state of the network across layers and vendors.

Open APIs such as TAPI, WebSocket, and a variety of RESTful APIs are likewise used for communications northbound from the SDN controller to multi-domain orchestrators and OSS critical for multi-domain and end-to-end lifecycle management.

Transport Application Program Interface, or TAPI, release 2.0 was released by the Open Networking Forum (ONF) in late 2017. It is worth calling out because it is the de facto standard for communications northbound between optical domain controllers and the OSS or multi-domain orchestrators. It came out of the Telecom Infra Project Open Optical and Packet Transport (TIP OOPT) project group with a goal of standardizing the open transport SDN architecture and achieving vendor-agnostic network programmability.

TAPI defines the set of models for managing optical transport networks. These models cover equipment inventory, topology, connectivity service, fault, and performance. TAPI is used by external systems and does not define the southbound interface (SBI) between the controller and the device.

INTEGRATED ANALYTICS INFORM BETTER DECISIONS

Software control and automation are essential to an adaptive network. Analytics must be able to collect traffic and performance data from all Layer 0–3 devices and then act on that information in an informed, coherent, and intelligent fashion. This requires the tight integration of analytics engines with the SDN controller.

The ability to gather data from Layers 0–3 enables the CSP to highlight capacity exhaustion along with underutilized resources. This is not a trivial task. As mentioned earlier in the report, the SDN controller is collecting telemetry data from a variety of devices from multiple vendors with different data formats. In order to achieve network lifecycle automation, the SDN controller must be able to apply AI/ML algorithms to the data collected on a real-time basis and then generate network insights and actions with minimal operator intervention.

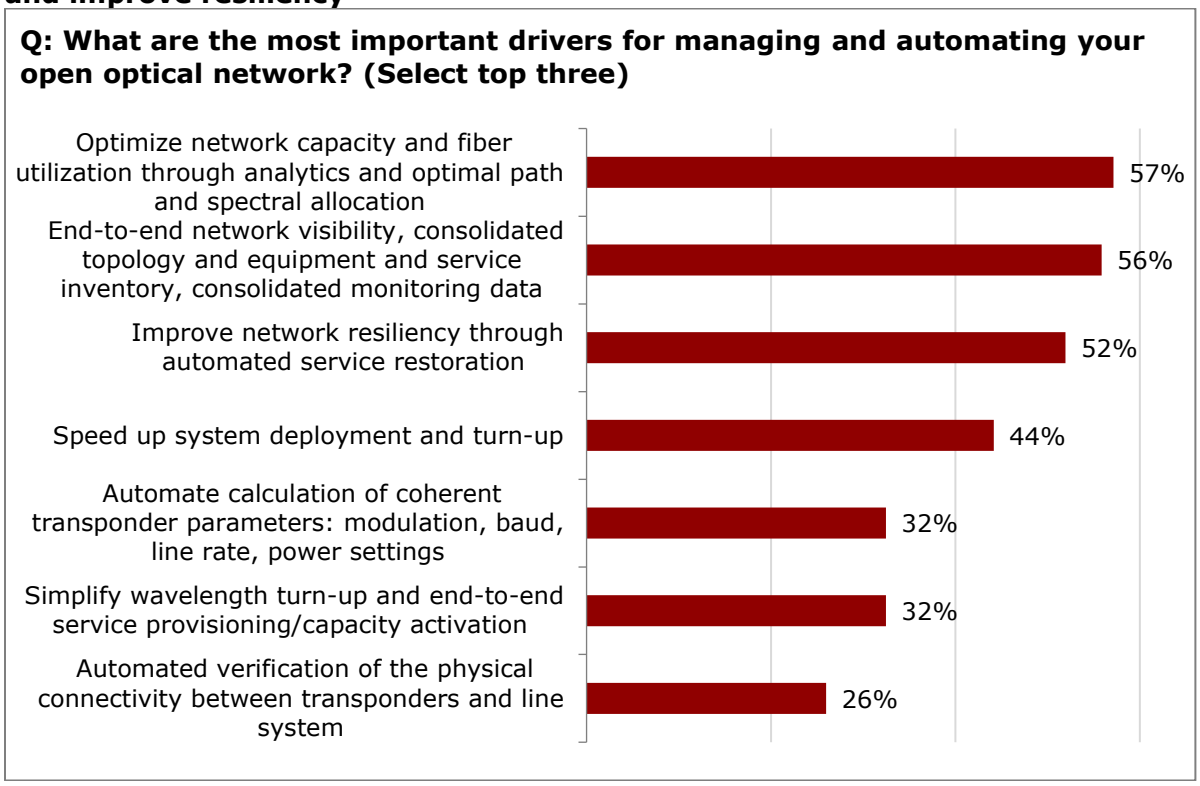
The coordinated, multi-layer performance optimization of IP and optical networks both simplifies and improves the following:

- **Network monitoring:** The CSP can troubleshoot IP or optical network issues quickly by leveraging both real-time performance data and historical data, correlated across Layers 0–3, and better predict future network requirements and the impact of network changes.
- **Service monitoring:** Service performance can be monitored against key performance indicators (KPIs), enabling the CSPs to meet monthly service-level agreements (SLAs) and avoid penalties.
- **Traffic engineering:** Network utilization metrics can be used to resolve link congestion and improve capacity planning. Information can be used to create active and backup paths based on network policies and network state, allowing CSPs to turn up services more quickly and to engineer the network for rapid recovery from network faults (for example, a fiber optic cable-cut).

The CSPs surveyed in Heavy Reading's Transport Automation Survey agree that the most important drivers to managing and automating their network are (see **Figure 5**):

- Optimized network capacity
- End-to-end network visibility
- Improved network resiliency

Figure 5: CSPs want to optimize network capacity, facilitate end-to-end visibility, and improve resiliency



n=77

Source: Heavy Reading, Transport Automation Survey 2022

CONCLUSIONS

The growth in the number of cell sites, coherent optical ports, connected devices, and IoT devices described at the beginning of this report might suggest that scalability is the most significant challenge the CSPs must deal with when it comes to managing their network infrastructure. However, networks do not scale gracefully or gradually. There are huge swings in demand driven by any number of forces: the sudden shift of the workforce from offices to a work-at-home model, the introduction of new applications, the shuttering or consolidation of regional enterprise offices, the widespread adoption of video conferencing and video calling, and the increased use of latency-sensitive augmented and virtual reality (AR/VR). The industry may be able to forecast the growth in devices or cell sites, but it cannot pinpoint where or when demand will hit. Given cost pressures, excess capacity cannot be built out in advance, particularly at the network edge, in a "just-in-case"

operational ethos. The network must be able to react to just-in-time capacity demand with speed and agility.

Enhanced and simplified network management is key. The adoption of SDN domain controllers as part of a standards-based, cloud native, multi-layer network improves network management in the following ways:

- **Operational efficiency:** Reduces opex and lead time in fulfilling customer requests and avoiding costly overbuilds.
- **Service agility:** Improves customer satisfaction and accelerates time to revenue.
- **Operations automation:** Realizes the potential of an adaptive network.

Domain-specific controllers provide the essential bridge between physical and virtual infrastructure elements and higher order multi-domain orchestration systems and OSS. By managing Layers 0 (the photonic or DWDM layer) through 3 as one unit, CSPs can simplify the management of their network. At the same time, they can take a giant step down the road toward operations automation and digital transformation. Multi-layer controllers should be a central element in an IT-based digital transformation journey.