SPECIAL TECHNICAL REPORT

Chris Granger

ORCHESTRATE WITH EASE

HOW PON TECHNOLOGY STREAMLINES THE TRANSITION TO SOFTWARE-DEFINED NETWORKING

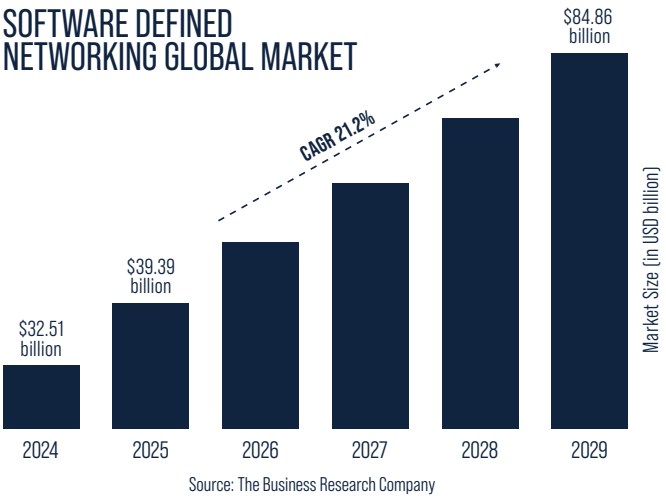
FEBRUARY 2026

ORCHESTRATE WITH EASE

HOW PON TECHNOLOGY STREAMLINES THE TRANSITION TO SOFTWARE-DEFINED NETWORKING

Today's networks are more complex than ever, with an ever-increasing number of devices, users, and applications distributed across diverse systems. This complexity presents significant challenges for IT departments grappling with budget constraints, staff shortages, and multiple vendors – all while striving to maintain high performance, robust security, and scalability.

Software-defined networking (SDN) emerges as an ideal solution for streamlining the management of complex, modern networks with large enterprises, government, and military entities at the forefront of adoption. Recent research predicts substantial growth in the global SDN market, from $32.5 billion in 2024 to nearly $85 billion in 2029, at a compound annual growth rate of 21.2%.[1]



While SDN offers the promise of streamlined IT operations, its successful implementation requires the right approach to avoid unnecessary costs and complications due to vendor lock-in, integration limitations, and scalability constraints. Passive Optical Networking (PON), which already inherently simplifies IT operations and lowers costs for local area networks (LANs), streamlines the transition to SDN, unlocking truly flexible and scalable "single-pane-of-glass" orchestration, all while sidestepping prohibitive costs and complexities.

WHAT IS SOFTWARE-DEFINED NETWORKING (SDN)?

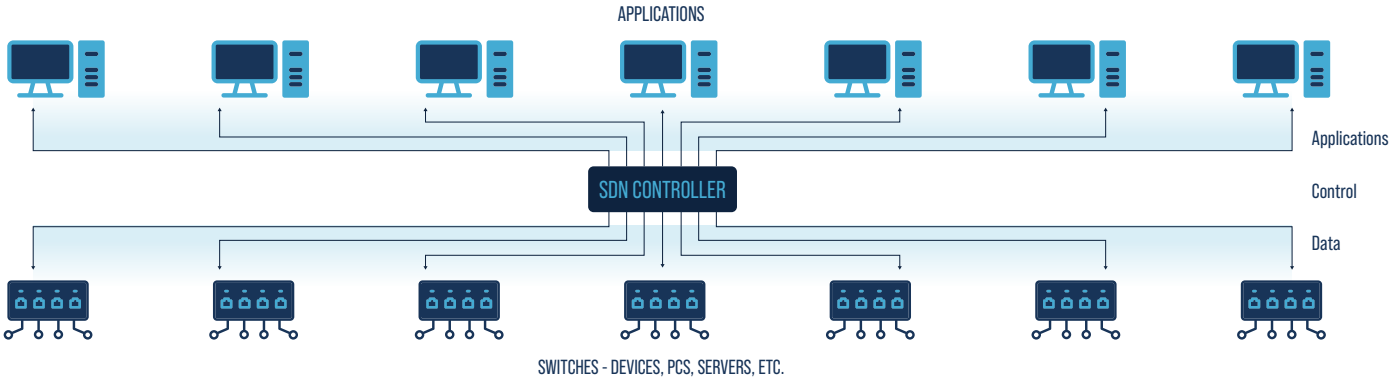
SDN separates the network control plane, which makes routing decisions, from the data plane, which forwards traffic based on those decisions. This abstraction from physical hardware enables centralized network control and management that streamlines IT operations and reduces costs through several key capabilities:

- **Automated provisioning and configuration:** SDN enables the automated configuration and setup of new network equipment, as well as uniform rollouts of software updates and other policies. This reduces IT staff workload, potential errors, and downtime while enabling faster, more cost-effective deployment of new services and applications
- **Dynamic resource allocation:** SDN enables allocation of bandwidth, load balancing, and traffic routing based on application requirements or service-level agreements (SLAs), ensuring optimal network performance and reliability.
- **Enhanced security and compliance:** By enforcing Zero Trust principles, as required by OMB M-22-09, SDN ensures that every user and device is continuously validated. Centralized control and real-time monitoring reduce the risk of cyberattacks, helping organizations stay compliant with the Federal Information Security Modernization Act (FISMA) and other federal security standards.

SDN originated in public switched telephone networks to simplify management and provisioning. As technology advanced, service providers adopted SDN as a means to make their networks programmable, enabling the deployment of new services and supporting diverse traffic patterns and workloads. They also recognized SDN's potential to move away from proprietary protocols and foster a more competitive, vendor-neutral environment by using a standardized control plane. The advantages of SDN made it an excellent fit for virtualized data centers, where it gained significant popularity for provisioning new equipment and managing routing, throughput, security, and other policies.

SDN principles were subsequently applied to wide-area networks (SD-WAN) and local area networks (SD-LAN) to enable centralized automated management, coordination, and provisioning of resources. While SD-WAN controls and encrypts traffic flows across geographically distributed networks (cloud, broadband, 4G/5G connectivity, etc.), SD-LAN provides centralized control over local switches, gateways, and wireless access points serving branch offices, campuses, and military bases. Integrating SD-LAN with SD-WAN offers seamless centralized network management and visibility across an entire branch network environment.

1. *Software Defined Networking Global Market Report 2025, The Business Research Company*



NEXT GENERATION ORCHESTRATION

The increasing complexity of networks has led to the introduction of higher-level SDN orchestration platforms that offer a transformative approach to managing multiple SDN environments. SDN orchestration platforms sit above and instruct SDN controllers, acting as a central full-service orchestrator for automating the provisioning and management of network resources across multiple systems and technologies.

SDN orchestration platforms may be developed internally by an organization or delivered through third-party providers, either on-premises or in the cloud. Cloud-based orchestrators offer flexibility and scalability, while also driving innovation through the use of artificial intelligence (AI) and machine learning (ML). These capabilities go beyond basic automation by enabling anomaly detection, predictive capacity management, and adaptive Zero Trust policy enforcement, helping organizations anticipate issues, optimize resources, and continuously align with security and mission needs.

One emerging approach to SDN involves using a cloud-native secure access service edge (SASE) framework that provides a single platform for network orchestration and security services, such as Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and firewall as a service (FWaaS). With SASE, all devices and users, regardless of their location, connect through the cloud-based platform to gain secure access.

SASE addresses the growing shift towards remote work, mobile access, and cloud adoption, enabling improved visibility, security, and control over traffic across all ports and protocols. By integrating Zero Trust Network Access (ZTNA) as a core component, SASE ensures that every connection, regardless of location or device, is continuously authenticated and authorized. As these newer SASE offerings evolve to address regulatory compliance and integrate seamlessly with existing systems, they provide an optimized foundation for enterprise-wide manageability and security. Like cloud-based orchestrators, SASE platforms also deliver flexibility and scalability, leveraging AI/ML to enhance security and performance.

NAVIGATING SD-LAN CHOICES

Choosing the right SD-LAN solution is a strategic decision that can significantly impact the future of your network. Careful planning and consideration of an organization's unique priorities can unlock greater agility, efficiency, and innovation. Key aspects to explore when choosing a solution include:

- **Integration:** Prioritize solutions that offer interoperability and seamless integration with existing systems, including legacy infrastructure, to minimize disruption and maximize return on investment.
- **Flexibility:** Seek options with flexible programmability and management capabilities that enable comprehensive end-to-end SDN to support diverse applications, networks, policies, and environments.

Traditional LAN	Passive Optical LAN (POL)
Hundreds of access switches, each with its own IP address	Few OLTs manage thousands of ONTs (unmanaged devices)
Complex, layered architecture (access → aggregation → core)	Flat, simplified architecture with centralized control
High space, power, cooling needs	Lower space, power, cooling requirements
Many devices to patch, license, and secure	Fewer devices, simpler patching and security
Larger attack surface	Reduced attack surface, fewer points of vulnerability

- **Scalability:** Select a solution that can confidently support both current and future network demands, accommodating expanding user bases, increasing device numbers and types, faster transmission speeds, and greater workloads.
- **Security:** Choose solutions with robust security protocols, including strong authentication, encryption measures, and advanced detection capabilities to prevent unauthorized access, mitigate vulnerabilities, and safeguard against cyberattacks.
- **Cost:** Evaluate overall capital and operational expenditure, including upfront costs, licensing fees, and the need for internal expertise and training to ensure an optimized and sustainable investment.

THE POWER OF OPEN-SOURCE SDN SOLUTIONS

The open-source landscape has significantly driven the evolution of SDN. Introduced in 2008, OpenFlow emerged as the first standard command line interface (CLI) protocol for SDN architecture. It established a communication bridge between the control and data planes of a network, using flow-based forwarding with flow tables that define how switches manage traffic. As an open standard, OpenFlow played a pivotal role in early SDN implementations, enabling a multi-vendor environment. This meant SDN software could control any OpenFlow-enabled network switch or router from any vendor, empowering network operators to centrally orchestrate and manage devices across the network.

While OpenFlow gained early momentum in data center environments, especially OpenStack cloud-based operating systems, it encountered challenges with scalability as networks and bandwidth rapidly expanded. Additionally, many network equipment vendors were reluctant to fully embrace the protocol due to concerns about relinquishing control.

The evolution of open-source SDN continued with the introduction of additional standardized API protocols for centralized configuration, such as Yang-based NETCONF (Network Configuration), RESTCONF (Representational State Transfer Configuration), and gRPC Network Management Interface (gNMI). NETCONF utilizes common XML language to securely send, retrieve, copy, and edit network device configuration information. RESTCONF, a more modern (REST)-like protocol, offers NETCONF functionality with HTTP-based web-friendly operation. gNMI is a Google Remote Procedure Call (gRPD) protocol for managing network devices. These Yang-based open protocols champion a vendor-agnostic “white-box” approach to networking, which enables the separation of hardware and software. This allows the data plane to remain simple and focused on its primary focus of efficiently routing data packets and maintaining throughput. At the same time, more complex functions are handled at higher layers. This approach offers faster deployment, enhanced scalability, improved performance, and better security.

Application programming interfaces (APIs) based on open protocols like NESCONF, RESCONF, and gNMI are vital to the success of SDN, ensuring interoperability and allowing controllers to communicate and interact with various network systems and hardware. Southbound APIs enable connections between controllers and network equipment (switches and routers). Northbound REST APIs allow various business applications to communicate their network needs to controllers. For instance, northbound REST APIs are essential for seamlessly integrating firewalls, intrusion detection systems, surveillance and monitoring systems, load balancers, and wireless and media gateways.

An open-source approach using published APIs is also essential for next generation orchestration and SASE platforms to manage any network, as well as any application or service that runs on those networks. APIs can even enable orchestration of both software-defined IT and operational technology (OT) systems, paving the way for secure and reliable IT-OT convergence. Through APIs, orchestration platforms can consolidate control and monitoring, enforce security policies, and manage the flow of data across IT and OT networks. This SDN approach is being embraced by mission-critical utility and manufacturing infrastructure.[2]

EXPLORING PROPRIETARY SDN SOLUTIONS

Some traditional Ethernet switch vendors have introduced their own proprietary SDN solutions, leading to a more fragmented landscape. While these solutions support northbound APIs for application integration in an SD-LAN, they involve tightly coupled controller software and network hardware from a single vendor, requiring support for proprietary mechanisms across equipment in lower-level network data planes. This can lead to vendor lock-in, hindering integration and scalability in mixed-vendor networks and diverging from the white-box, open-source, and standards-based vision of SDN that keeps the data plane simple. Proprietary SDN solutions also typically have higher initial costs, ongoing licensing fees, and a steep learning curve for untrained personnel that can increase capital and operational expenses.

2. *Applying SDN and Automation Technology to Critical Infrastructure, Juniper Networks*

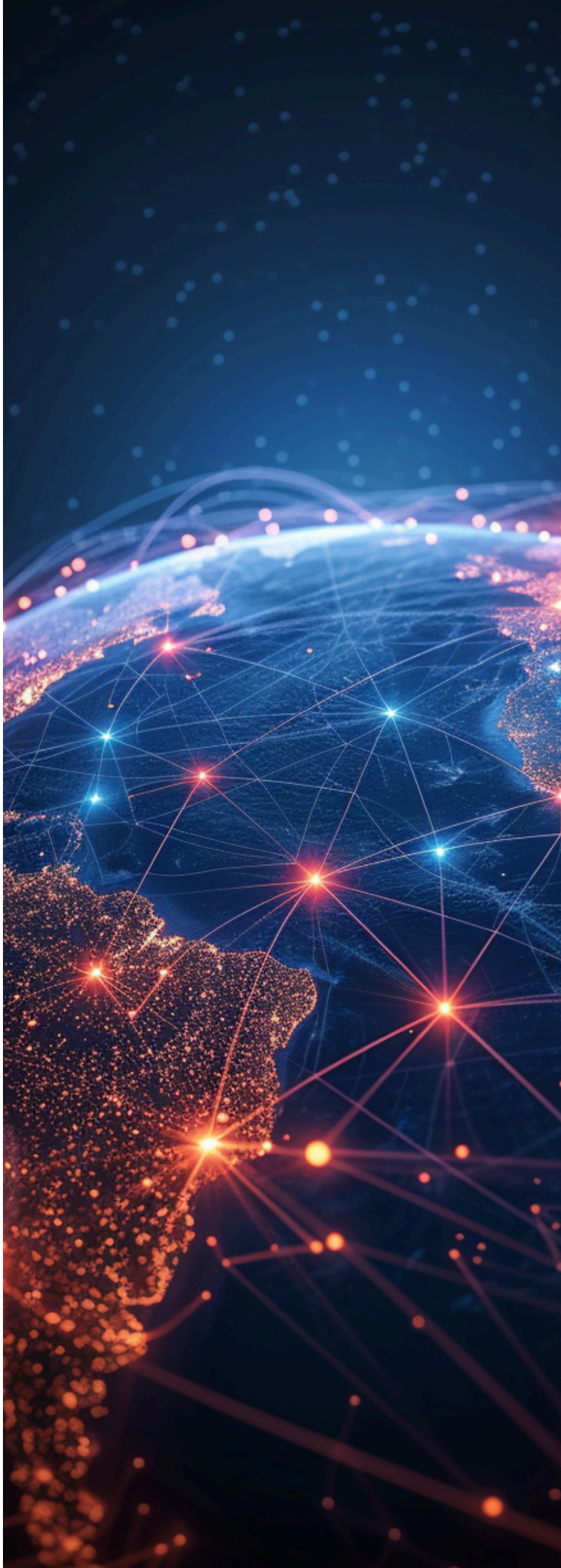
Some proprietary SDN solutions are deployed as an overlay, essentially creating a virtual network on top of an existing infrastructure. In an overlay system, logical networks are established through secure, encrypted tunnels between endpoints that an SDN controller manages. While overlay systems can help organizations leverage SDN without expensive LAN upgrades, they may leave inherent underlying reliability issues, complexity, and security gaps in the existing network unaddressed.

PASSIVE OPTICAL LANS ARE SD-LANS

PON technology, initially developed for Fiber to the Home (FTTH or FTTX) networks, has always been inherently SDN capable due to its centralized architecture – it does not utilize SDN as an overlay on top of an existing network. In the service provider sector, the escalating demand for high quality of service (QoS) has made FTTX networks increasingly complex to manage. To address this, service providers have increasingly relied on PON's SDN capabilities to activate services efficiently, customize offerings to meet individual subscriber needs, and manage and monitor subscriber traffic flows for an improved quality of experience. All of these functions are performed across millions of widely distributed ports from a single management system, all with zero-touch operation from service providers. Now, as PON technology expands in the enterprise space to support passive optical LANs, it brings its inherent SDN functionality to organizations across all sectors, including government and military entities.

In a software-defined passive optical LAN, the optical line terminal (OLT) acts as the controller. The optical network terminals (ONTs) that provide connectivity for users and devices do not store any information and are controlled exclusively by the OLT, keeping the data plane simple and shifting more complex functions to the OLT. Like "white box" access switches in an open, vendor-agnostic switched network, simple, unmanaged ONTs are best suited for SDN rather than complex, full-functioning traditional switches.

The OLT distributes configuration information to individual ONT ports, assigning security attributes such as VLAN, 802.1X port authentication, encryption, network access control, as well as bandwidth, QoS, power over Ethernet (PoE), and Link Layer Discovery Protocol (LLDP) for inventory. This entire process can be automated using templates and profiles in the OLT, enabling machine-to-machine (M2M) actions for dynamically allocating resources on a per-service, per-port, per-end-device, and per-user basis according to real-time needs and SLA attributes.



Multiple distributed passive optical LANs can also be managed via a PON web-based centralized management platform that leverages SDN, essentially acting as an orchestration platform. This allows network operators to view and configure all OLTs, ONTs, and ONT ports from a single location—regardless of whether they are located across a campus, a region, a state, a country, or even in international locations. Policy consistency is maintained through global templates and profiles created in the management platform, which can be assigned to multiple OLTs to automatically configure individual ONTs, significantly reducing the likelihood of misconfigurations that can lead to network disruptions, performance issues, or security gaps.

With complete visibility of the entire network down to the port level, the PON management platform can also log every event, from the addition of a new ONT on the network to PoE usage on a port and even user logins and logouts. Through a PON management platform, network operators can also distribute software upgrades to OLTs and set system-level parameters, such as scheduled backups, inventory tracking, and alarm settings. Passive optical LANs also support the use of automation scripts, which are sequences of instructions for automating repetitive tasks that help accelerate commissioning, reconfigurations, and troubleshooting, while further minimizing human error and security risks.

When a new device connects, the system can automatically detect, authenticate and validate it, apply the correct access profile (security, VLAN, QoS, etc.), grant network access, and log all actions for visibility and compliance.

OPTIMIZED FOR NEXT-GEN SD-LAN

Passive optical LANs that inherently function as SD-LANs also leverage the right approach to significantly simplify the transition to advanced third-party orchestration and SASE platforms, empowering IT teams to enhance reliability and strengthen security across multiple, distributed wired and wireless networks.

Open-Source Orchestration Support

A key advantage of a passive optical LAN is its robust support for open-source orchestration. This vendor-agnostic approach relies on standardized protocols for configuration, security, management, provisioning, and monitoring. As a result, passive optical LAN OLTs and management platforms easily integrate into mixed-vendor environments and effectively support third-party orchestrators and future SASE platforms through these standard protocols:

- YANG-based NETCONF, RESTCONF, and gNMI for configuring OLTs and ONTs
- RADIUS (Remote Authentication Dial-In User Service) protocol to manage authentication, authorization, and accounting for users connecting to the network
- ZTP (Zero Touch Provisioning) for automatic setup and initial configuration of OLTs (IP address, DNS, PKI certificate, etc.)
- SMNPv2/SMNPv3 for monitoring and managing devices and network telemetry
- Syslog for log management, security event management, and service desk ticketing

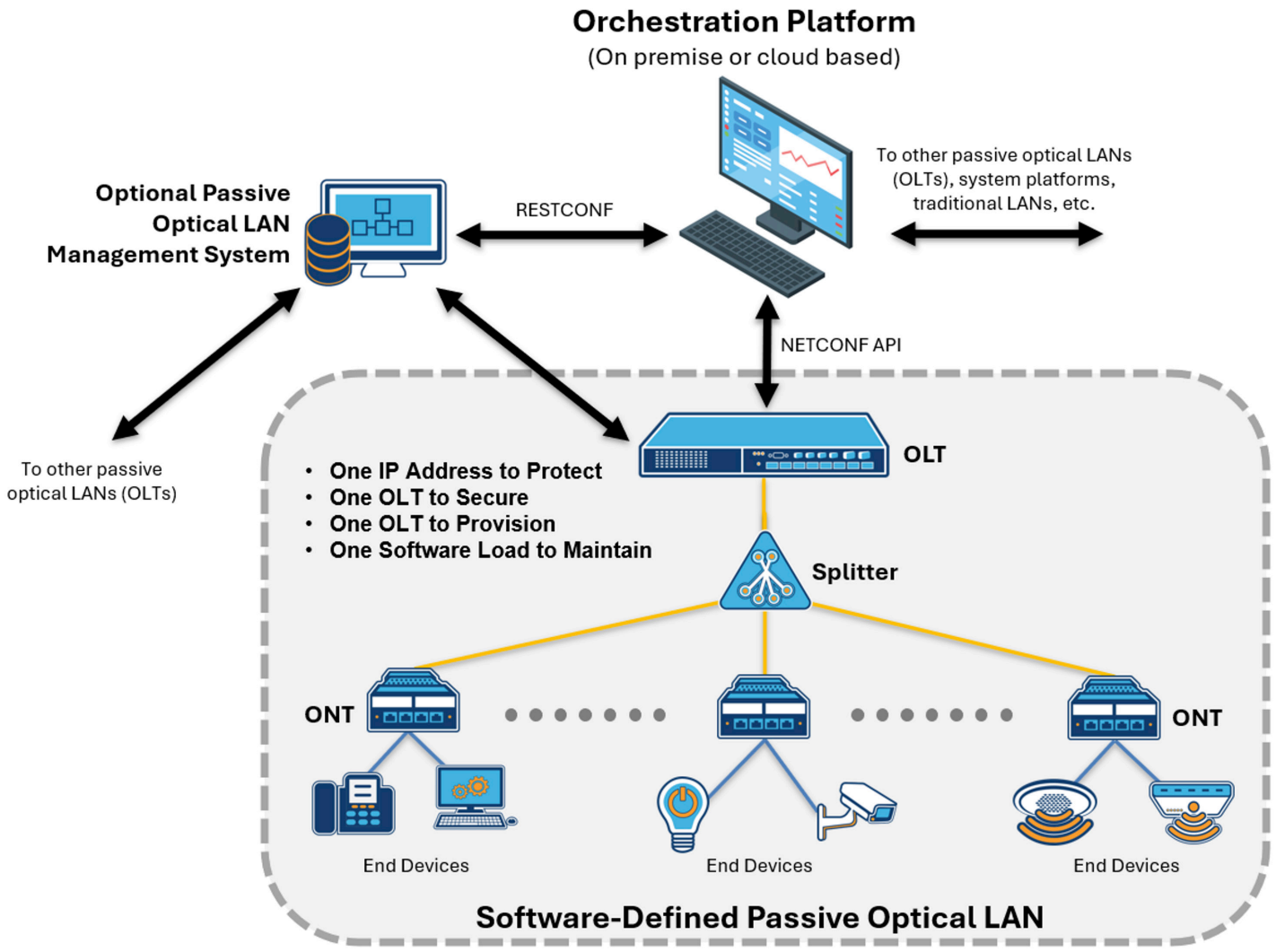
By utilizing these standardized protocols, passive optical LANs can communicate vital information about network performance, security, and compliance, facilitating informed decision making and issue detection. This includes role-based access, controlling who has permission to access and configure network services through the orchestration platform. While a centralized passive optical LAN management system acts as its own orchestrator, advanced OLTs also incorporate APIs to integrate directly with third-party orchestration and SASE platforms.

Furthermore, passive optical LANs support the use of playbooks based on common programming languages. These playbooks create automation workflows within an orchestration platform, defining how network services should be provisioned, modified, and decommissioned. They can generate a list of devices for standard tasks, such as security hardening policies, QoS settings, and routing configurations, effectively automating mission-critical yet repetitive operational tasks and significantly reducing the need for IT staff and associated costs.

REDUCED DATA PLANE COMPLEXITY

The overall design of a passive optical LAN further simplifies SDN by reducing the complexity of the data plane compared to traditional, often proprietary, switched networks. In a passive optical LAN, unmanaged ONTs support a “white box” approach to SDN, which keeps the data plane simple and focused on routing data packets and maintaining throughput, while facilitating network scalability and avoiding vendor lock-in. This simplicity also translates to significant cost reductions and more streamlined operation by eliminating hundreds or even thousands of traditional switches.

In a passive optical LAN, only the OLT requires an IP address for management purposes. A single OLT (or a pair of OLTs for redundancy) can be sized to support



8,000 or more connections via ONTs. In contrast, a traditional switched network would require around 300 access switches, each with its own IP address, to support the same number of connections. This significantly reduces equipment installation costs, as well as space, power, and cooling requirements. Operational costs are further minimized by reducing downtime, inventory, and licensing fees with fewer active components. Fewer active devices also reduce the time spent on network troubleshooting, moves, adds, and changes, thereby reducing IT staff and training needs and shifting the operational focus to more mission-critical tasks.

With substantially fewer devices to provision, manage, and secure, passive optical LANs greatly simplify SDN. Only the OLT has to be configured, managed, and secured, as it centrally manages all connected ONTs. In a traditional switched network, every aggregation and access switch must be individually licensed, configured, managed, and secured. Having far fewer complex full-functioning devices also means fewer points of vulnerability, thereby reducing the attack surface and minimizing the risk of malicious and negligent human errors.

From an ongoing operational standpoint, an SD-LAN orchestrator would need to manage and optimize a traditional switched network using status and performance information (e.g., bandwidth utilization, packet loss, Syslog, SNMP traffic, etc.) gathered from hundreds or thousands of switches. In contrast, an entire passive optical LAN can be managed and optimized based on information from just one OLT.

THE CLEAR ADVANTAGE

Passive optical LANs are already recognized for their ability to simplify IT operations and significantly reduce costs by eliminating hundreds or even thousands of switches and their associated space, power, and cooling requirements. Organizations embarking on the transition to advanced SDN orchestration platforms or exploring emerging SASE platforms to manage ever-increasingly complex networks gain a clear advantage with software-defined passive optical LANs.

The inherent design of a passive optical LAN, which leverages open, standards-based protocols and requires far fewer interfaces and IP addresses to manage, streamlines SDN deployment, empowering a more flexible and scalable "single-pane-of-glass" orchestration. This revolutionizes network control, allowing organizations across all verticals to adapt, innovate, and optimize their systems with unprecedented effectiveness.

In summary, software-defined passive optical LANs offer the following benefits:

- **Open, standards-based integration:** Avoids costly vendor lock-in and seamlessly integrates with multi-vendor networks and third-party orchestration and SASE platforms through standardized protocols.
- **Streamlined orchestration:** Provides comprehensive visibility and control down to the port level, from a single management platform, enabling efficient automation and policy consistency across distributed networks.
- **Reduced data plane complexity:** Simplifies the network by utilizing simple ONTs and centralizing control at the OLT, enabling a "white box" approach.
- **Fewer points to manage:** Drastically reduces the number of devices (IP addresses and CLIs) requiring configuration, security, and ongoing management compared to traditional switched networks.
- **Enhanced security:** Fewer active components and centralized control reduce points of vulnerability and the potential for human error.

ABOUT THE AUTHOR

Chris Granger is a senior IT executive and U.S. Marine Corps veteran with over 30 years of federal and DoD experience. He most recently served as the Acting Deputy CIO and Executive Director of IT Operations at DHS, leading major cybersecurity and modernization initiatives. He is the founder of Spartan Technology LCC, an SDVOSB consultancy, and continues to advise government and industry leaders on digital modernization, Zero Trust, and secure network architecture.