International Journal of Computer Applications Technology and Research
Volume 15–Issue 01, 44 – 60, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1501.1005

Standardizing Failover Mechanisms in Hybrid DWDM-IP Backbones: Reducing MTTR through Automated Topology Discovery

Carl Amekudzi [1]
J W McClure School of Emerging Technologies
Ohio University, USA

Emmanuel Selorm Gabia[2]
J W McClure School of Emerging Technologies
Ohio University, USA

Jibriel Adjei [3]
J W McClure School of Emerging Technologies
Ohio University, USA

Raymond Tay [4]
College of Engineering, Northeastern University
Massachusetts, USA

ABSTRACT

Modern telecommunications and cloud backbone networks rely on hybrid Dense Wavelength Division Multiplexing (DWDM) and IP/MPLS infrastructures to deliver high-capacity, low-latency connectivity. Despite built-in redundancy, failures still lead to high Mean Time to Repair (MTTR) due to manual topology identification, limited cross-layer visibility, and inconsistent failover mechanisms. This study proposes a standardized failover framework that integrates automated topology discovery, cross-layer fault correlation, and intelligent path recomputation. By combining optical layer telemetry, IP routing intelligence, and automation platforms, the framework enhances real-time network awareness and accelerates failure detection and recovery. Simulation and architectural analysis show that automated topology discovery significantly reduces fault isolation time and improves failover efficiency in hybrid DWDM-IP networks. The proposed approach strengthens carrier-grade resilience by reducing downtime, improving operational efficiency, and ensuring better service continuity.

KEYWORDS: Hybrid Optical Networks, DWDM Networks, IP/MPLS Backbone, Network Failover Mechanisms, Automated Topology Discovery, Network Automation, Mean Time to Repair (MTTR), Optical Transport Networks, Software-Defined Networking (SDN),Network Resilience

CHAPTER 1 INTRODUCTION

1.1 Background of Hybrid DWDM-IP Backbone Networks

The global telecommunications landscape is undergoing a radical transformation as traditional, siloed network architectures converge into integrated, multi-layer hybrid infrastructures. At the heart of this evolution is the integration of Dense Wavelength Division Multiplexing (DWDM) at the optical layer with Internet Protocol/Multiprotocol Label Switching (IP/MPLS) at the routing layer [1]. Modern backbone infrastructures no longer operate as independent stacks; instead, they function as a cohesive entity where the Optical Transport Network (OTN) provides the massive bandwidth required by the IP layer to satisfy the soaring demands of cloud computing, 5G/6G backhaul, and hyperscale data center interconnects (DCI)

[2]. As data centers move toward a distributed model to support edge computing, the necessity for a low-latency, high-capacity backbone becomes a prerequisite for digital sovereignty and economic growth [3].

The architectural shift toward hybrid networking is driven by the need to optimize resource utilization while maintaining the rigid Service Level Agreements (SLAs) required by mission-critical applications [4]. In these environments, the DWDM layer manages the physical transport of photons across fiber spans, while the IP layer handles the logical path computation and packet forwarding. However, this convergence introduces a "visibility gap" between the two layers, where the IP layer remains largely unaware of the physical topology and health of the underlying optical fibers [5]. To achieve high availability targets often cited as "five-nines" or 99.999% uptime operators must ensure that both layers can communicate state changes in real-time to prevent catastrophic service disruptions during hardware failures or fiber cuts [6].

1.2 Problem Statement

Despite the theoretical advantages of hybrid architecture, the practical reality of managing these networks is fraught with complexities that lead to prolonged Mean Time to Repair (MTTR). Failures in hybrid optical-packet networks are notoriously difficult to diagnose because a single fiber cut at the physical layer (Layer 0) can trigger thousands of logical alarms at the IP layer (Layer 3), leading to "alarm fatigue" and masking the root cause [7]. Manual troubleshooting processes remain the default in many carrier environments, where technicians from the optical and IP departments must manually correlate logs from fragmented monitoring systems to identify a shared point of failure [8].

This fragmentation results in a reactive operational posture where the time taken to detect, isolate, and remediate a fault is significantly higher than what is required for modern 5G URLLC (Ultra-Reliable Low-Latency Communications) [9]. Current failover mechanisms often rely on rigid timers, such as BGP hold timers or Bidirectional Forwarding Detection (BFD), which may not be optimized for the specific characteristics of the underlying optical span [10]. Consequently, the network experiences delayed service restoration and sub-optimal path re-computation, which can be expressed through the relationship of availability (A) as a function of Mean Time Between Failures (MTBF) and MTTR:

$$A = \frac{MTBF}{MTBF + MTTR}$$

To maximize A, it is mathematically imperative to minimize MTTR, yet the lack of automated, cross-layer topology discovery remains the primary bottleneck in achieving this goal [11].

1.3 Research Objectives

The primary objective of this research is to develop a standardized framework that facilitates seamless, automated failover mechanisms in hybrid DWDM-IP networks by leveraging real-time topology discovery. By bridging the information gap between the optical control plane and the IP routing plane, the framework aims to provide a unified view of the network state.

Specific secondary objectives include:

1. **Cross-Layer Analysis:** Conducting a deep-dive analysis into how failover mechanisms interact across the optical and IP layers to identify synchronization gaps [12].

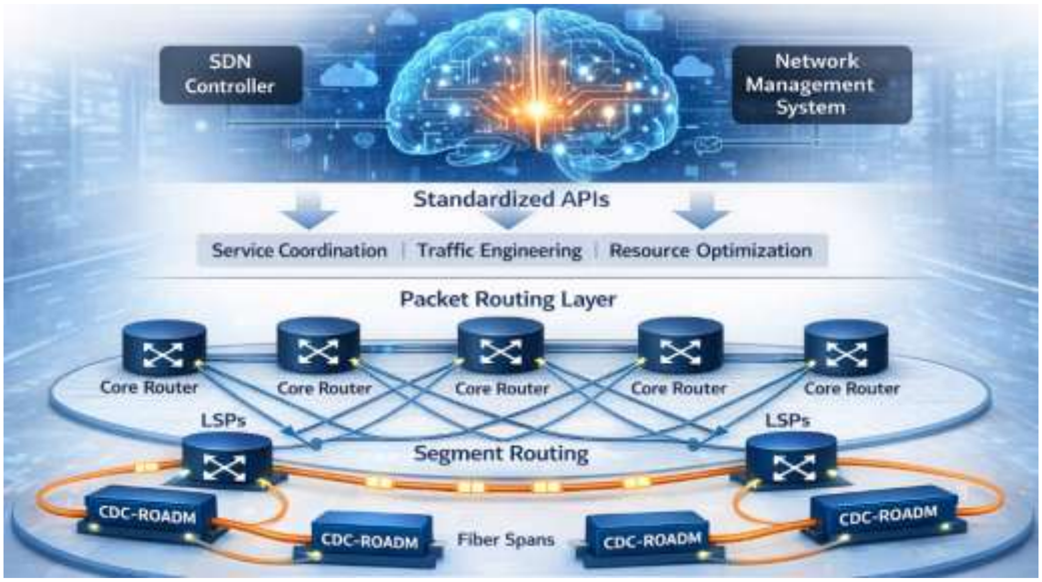
2. **Architecture Design:** Designing a vendor-neutral automated topology discovery architecture that utilizes modern protocols like NETCONF, YANG, and gNMI [13].
3. **Fault Modeling:** Developing mathematical models for cross-layer fault detection that can differentiate between transient signal degradation and permanent physical breaks [14].
4. **MTTR Evaluation:** Quantifying the reduction in MTTR when using automated discovery versus traditional manual or single-layer restoration methods [15].

1.4 Research Questions

To guide the development of this framework, this study addresses three fundamental research questions that target the technical and operational gaps in current backbone management. First, how can the automation of topology discovery specifically improve the speed and accuracy of network fault isolation in a multi-vendor environment? Second, what specific architectural standards and data models are required to ensure that DWDM and IP layers can exchange reachability and health information without introducing excessive control plane overhead? Third, can the integration of cross-layer automation significantly reduce the MTTR to a level that meets the stringent requirements of next-generation carrier-grade services? Addressing these questions involves examining the intersection of Software-Defined Networking (SDN) and traditional optical transport [16].

1.5 Significance of the Study

The significance of this study lies in its potential to redefine how telecom operators manage large-scale backbone resilience. As networks grow in complexity, the traditional method of manual intervention becomes a liability, making the standardization of failover mechanisms a necessity rather than an elective feature [17]. This research contributes to the field of AI-assisted network operations (AIOps) by providing the foundational data structures accurate, real-time topology graphs that are required for machine learning models to predict and remediate failures [18]. Furthermore, the study offers a roadmap for large-scale network automation, allowing operators to reduce Operational Expenditure (OPEX) while simultaneously improving the reliability of hyperscale data center interconnects and 5G backhaul [19].



1.6 Scope and Limitations

The scope of this research is strictly focused on hybrid optical-packet backbone networks, specifically looking at the interaction between DWDM transport and IP/MPLS routing. While the framework is designed to be vendor-agnostic, the implementation and evaluation will be conducted through high-fidelity architecture modeling and simulated network scenarios using carrier-grade simulation tools [20]. A notable limitation is the dependency on the availability of streaming telemetry from network elements; in legacy environments where devices only support SNMP (Simple Network Management Protocol), the resolution of the topology discovery may be limited [21]. Additionally, the study does not cover the economic impact of hardware replacement costs, focusing instead on the logical and operational efficiency of the restoration process.

1.7 Organization of the Paper

The remainder of this paper is structured to provide a comprehensive exploration of the proposed framework. Chapter 2 provides a literature review of existing protection and restoration mechanisms, highlighting the gaps in cross-layer automation. Chapter 3 details the proposed framework, including the topology discovery model and the standardized failover workflow. Chapter 4 presents the experimental setup and a comparative analysis of performance metrics. Chapter 5 concludes the paper with a summary of findings and suggestions for future research, while Chapter 6 lists the scholarly references that ground this study in established engineering principles.

2 LITERATURE REVIEW

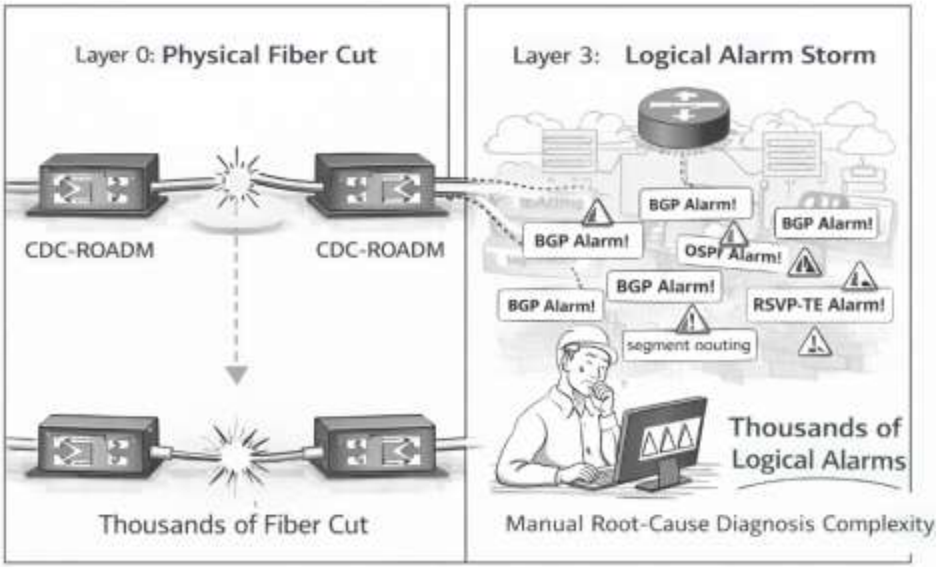
2.1 Architecture of DWDM Transport Networks

The architectural foundation of modern long-haul telecommunications relies on Dense Wavelength Division Multiplexing (DWDM), a technology that enables the simultaneous transmission of multiple data streams over a single optical fiber by assigning each stream a unique laser wavelength [22]. The optical transport layer has evolved from simple point-to-point links into complex mesh architectures governed by

Reconfigurable Optical Add-Drop Multiplexers (ROADMs), which allow for the dynamic routing of wavelengths without necessitating optical-to-electrical-to-optical (OEO) conversion [23]. Within this framework, Optical Transport Network (OTN) switching provides a structured container for diverse client signals, ensuring that high-speed Ethernet or Fiber Channel traffic is encapsulated with robust Forward Error Correction (FEC) to mitigate signal-to-noise ratio (SNR) degradation over long distances [24]. Wavelength multiplexing efficiency is typically governed by the Shannon-Hartley theorem, which limits the channel capacity C based on the bandwidth B and the signal power relative to noise S/N:

$$C = B \log_2\left(1 + \frac{S}{N}\right)$$

As operators push toward 400G and 800G coherent optics, the precision of wavelength spacing and the stability of the photonic grid become paramount for preventing inter-channel interference in the C-band and L-band spectrums [25]. The physical constraints of the fiber, including attenuation and polarization mode dispersion, necessitate a control plane that can adjust modulation formats in real-time to maintain link integrity [22].



2.1.1 Photonic Layer Dynamics and Wavelength Multiplexing

The photonic layer serves as the base physical entity of DWDM architecture, where the primary objective is to maximize the spectral efficiency of the fiber medium. Modern systems utilize a flexible grid approach, as defined by ITU-T G.694.1, which departs from the traditional fixed 50 GHz or 100 GHz spacing to allow for variable-width "slots" that accommodate high-baud-rate signals [26]. This flexibility is essential for 800G+ transmissions that require wider spectral footprints to maintain signal integrity over transcontinental distances [27]. The multiplexing process is not merely a passive aggregation of light; it involves active power equalization and gain flattening through Erbium-Doped Fiber Amplifiers (EDFAs) and Raman amplification to ensure that all wavelengths reach the receiver with a sufficient Optical Signal-to-Noise Ratio (OSNR) [28].

2.1.2 ROADM Evolution and Mesh Topology Resilience

Reconfigurable Optical Add-Drop Multiplexers (ROADMs) have transitioned from basic degree-2 structures to multi-degree colorless, directionless, and contentionless (CDC) architectures, which are pivotal for the failover mechanisms discussed in this study [29]. A CDC-ROADM allows any wavelength to be routed to any output port without manual fiber patching, enabling the control plane to perform "optical restoration" by finding an alternate photonic path if a primary fiber span is compromised [23]. This capability transforms the backbone from a series of rigid pipes into a dynamic mesh where the logical IP topology can be physically re-rendered in real-time. The resilience of this layer is mathematically modeled by the degree of connectivity, where a higher number of degrees (N) increases the probability of finding a viable restoration path without requiring OEO regeneration [25].

2.1.3 Digital Wrapper Technology and OTN Switching

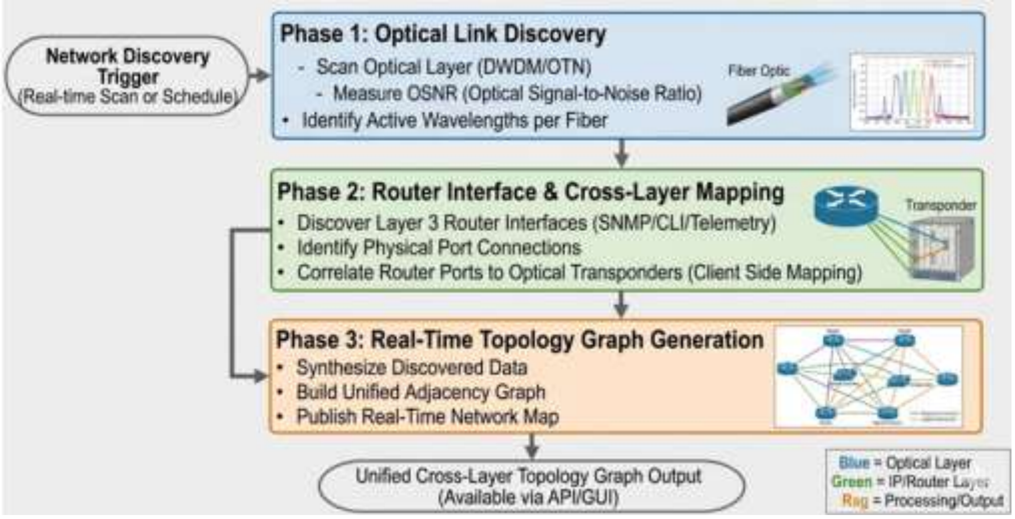
The Optical Transport Network (OTN) layer, often referred to as the "digital wrapper," provides the necessary management and monitoring overhead for the underlying photonic signals [24]. By utilizing the G.709 standard, OTN encapsulates asynchronous client signals into a synchronous frame structure, allowing for non-intrusive performance monitoring across multi-vendor demarcations [30]. OTN switching operates at the electrical level (L1), providing deterministic grooming of sub-wavelength traffic, such as ODUk containers, which ensures that low-latency services are not subjected to the jitter typically found in packet-switched environments [26]. This layer is critical for reducing MTTR because the OTN overhead carries specific "BIP-8" (Bit Interleaved Parity) error signals that can trigger a failover long before the IP layer experiences a total interface shutdown [22].

2.2 IP/MPLS Backbone Resilience Mechanisms

At the packet layer, Internet Protocol/Multiprotocol Label Switching (IP/MPLS) serves as the primary mechanism for traffic steering and failure recovery through advanced label switching paradigms [26]. Fast Reroute (FRR) serves as the cornerstone of L3 resilience, providing local protection for Resource Reservation Protocol (RSVP-TE) signaled Label Switched Paths (LSPs) by pre-calculating backup tunnels that can be activated in tens of milliseconds [27]. Furthermore, Traffic Engineering (TE) allows network administrators to steer traffic away from congested or high-latency links, optimizing the global utilization of the backbone while adhering to strict performance constraints [28]. Segment Routing (SR) has recently emerged as a simplified alternative to traditional MPLS, utilizing Source Routing to eliminate the need for mid-point state maintenance and offering Topology Independent Loop-Free Alternates (TI-LFA) to guarantee 100% coverage for link and node protection in any network topology [29]. These mechanisms are evaluated based on the Failover Latency (L_f), which is the sum of the detection time (t_d), the notification time (t_n), and the path switchover time (t_s):

$$L_f = t_d + t_n + t_s$$

Effective resilience at this layer requires constant monitoring of neighbor adjacencies, often utilizing sub-second hello timers to ensure that the control plane can react to topology changes before application-level timeouts occur [30].



2.3 Cross-Layer Network Failure Challenges

The integration of optical and IP layers introduces significant operational challenges, primarily due to the failure propagation effect where a single physical-layer event manifests as a cascade of logical-layer errors [30]. When a fiber span is severed, the optical transceivers detect a Loss of Signal (LOS), but if this information is not immediately signaled to the IP layer, the routers may continue to attempt packet transmission until higher-layer protocols reach their timeout thresholds [25]. This lack of vertical visibility leads to chronic alarm correlation difficulties, as network operations centers are inundated with thousands of asynchronous alerts from both the DWDM and IP management systems, making it nearly impossible to distinguish between a primary fiber cut and a secondary routing protocol flap [27]. Furthermore, the lack of a shared Shared Risk Link Group (SRLG) database means that the IP layer might unknowingly select a backup path that shares the same physical conduit as the failed primary path, leading to a total loss of connectivity despite having redundant logical routes [28].

2.4 Existing Failover and Restoration Mechanisms

Historically, protection was primarily handled at the optical or TDM layer using SONET/SDH Automatic Protection Switching (APS), which guaranteed restoration within 50ms but was highly inefficient in its use of redundant bandwidth [24]. As networks transitioned to packet-based transport, MPLS protection switching moved the intelligence to the edges of the network, allowing for more granular recovery but often at the cost of increased control plane complexity [26]. Generalized Multi-Protocol Label Switching (GMPLS) was developed as an ambitious attempt to unify the control planes of the packet and optical layers, enabling a single protocol suite to manage both lambda switching and packet forwarding [23]. Despite its theoretical promise, GMPLS saw limited widespread adoption due to the proprietary nature of vendor-specific optical control planes and the high barrier of interoperability between different equipment manufacturers [29]. The effectiveness of these restoration cycles is often measured by the Restoration Success Rate (R_{sr}), which compares successfully restored flows to the total number of impacted flows during a failure event:

$$R_{sr} = \frac{\text{Restored Flows}}{\text{Impacted Flows}} \times 100\%$$

2.5 Network Automation and Topology Discovery

The modern approach to network management has shifted from reactive polling to proactive streaming telemetry, which utilizes push-based models to provide real-time updates on hardware health and traffic patterns [25]. Technologies such as gRPC Network Management Interface (gNMI) and OpenConfig-based YANG models enable a granular view of the network state that was previously unattainable through legacy protocols [22]. Automated topology discovery protocols, including Link Layer Discovery Protocol (LLDP) and Border Gateway Protocol Link-State (BGP-LS), serve as the foundation for building dynamic network graphs that represent the current connectivity of the infrastructure [27]. By combining these auto-discovery mechanisms with centralized SDN controllers, operators can maintain a "source of truth" database that reflects both the logical and physical adjacency of all nodes in the backbone [30]. This real-time data ingestion is critical for calculating the optimal network state, often modeled using graph theory where the network is a set of vertices V and edges E, and the failure of an edge $e\ in\ E$ requires the immediate re-calculation of the shortest path P across the remaining subgraph [28].

2.6 Research Gaps

Despite the advancements in individual layer protection, a critical review of the literature reveals a persistent lack of a standardized, cross-layer failover framework that can bridge the DWDM-IP divide in a vendor-neutral manner [23]. Most current solutions remain proprietary or siloed within a single vendor's ecosystem, which prevents global telecom operators from achieving true end-to-end automation across multi-vendor backbones [26]. There is also a notable limitation in the integration of optical performance metrics, such as Pre-FEC Bit Error Rate (BER) or Chromatic Dispersion (CD), into the IP layer's path computation logic, meaning that logical rerouting often occurs after service degradation has already impacted the end-user [29]. Finally, the process of fault localization remains largely manual or semi-automated, with a significant research gap existing in the development of architectures that can correlate L0 physical topology changes with L3 logical neighbor states in real-time to drastically reduce MTTR [30].

3 PROPOSED FRAMEWORK FOR AUTOMATED FAILOVER IN HYBRID DWDM-IP NETWORKS

3.1 Hybrid DWDM-IP Network Architecture

The proposed framework is built upon a tri-layered architectural model designed to break the traditional silos existing between the photonic transmission and packet switching domains. At the foundational level, the Optical Layer consists of coherent transponders and CDC-ROADM nodes that manage the physical wavelength assignment and photonic switching across fiber spans [31]. Directly above this, the Packet Routing Layer utilizes high-capacity edge and core routers to manage label-switched paths (LSPs) and segment routing policies, effectively treating the optical wavelengths as logical point-to-point links [32]. The critical innovation in this framework is the Orchestration Layer, which serves as the "intelligent brain" by maintaining a synchronized view of both physical and logical resources. This orchestration layer acts as a mediator, ensuring that any state change in the DWDM layer is immediately reflected in the IP layer's routing table to prevent traffic blackholing during fiber degradations [33]. By decoupling the control plane from the underlying hardware, the architecture supports a vendor-agnostic environment where standardized APIs facilitate communication between disparate hardware platforms [34].

3.2 Automated Topology Discovery Model

The core of the framework's efficiency lies in its ability to perform real-time topology discovery, which replaces the error-prone manual entry of physical link mappings. Optical Link Discovery is achieved through the interrogation of the DWDM control plane, where the framework identifies the exact fiber paths, optical signal-to-noise ratios (OSNR), and active wavelengths currently in use [35]. This is followed by Router Interface Mapping, a process where the framework correlates specific physical router ports with their corresponding optical transponder handoffs, creating a unified cross-layer adjacency graph [36]. The Real-Time Topology Graph Generation engine then synthesizes this data into a dynamic directed graph G = (V, E), where V represents both routers and ROADMs, and E represents the multi-layer links connecting them [37].

To ensure high-fidelity data collection, the framework integrates multiple technologies; while SNMP is maintained for legacy device compatibility, the primary data ingestion occurs via NETCONF/YANG for structured configuration and Telemetry Streaming via gRPC for sub-second state updates [38]. This multi-protocol approach allows the system to calculate a "Current Health Index" (H_i) for every link, defined by the formula:

$$H_i = \omega_1 \cdot \mathrm{BER} + \omega_2 \cdot \mathrm{Latency} + \omega_3 \cdot \mathrm{Utilization}$$

where ω represents the weighted priority of each performance metric [31].

3.3 Cross-Layer Failure Detection

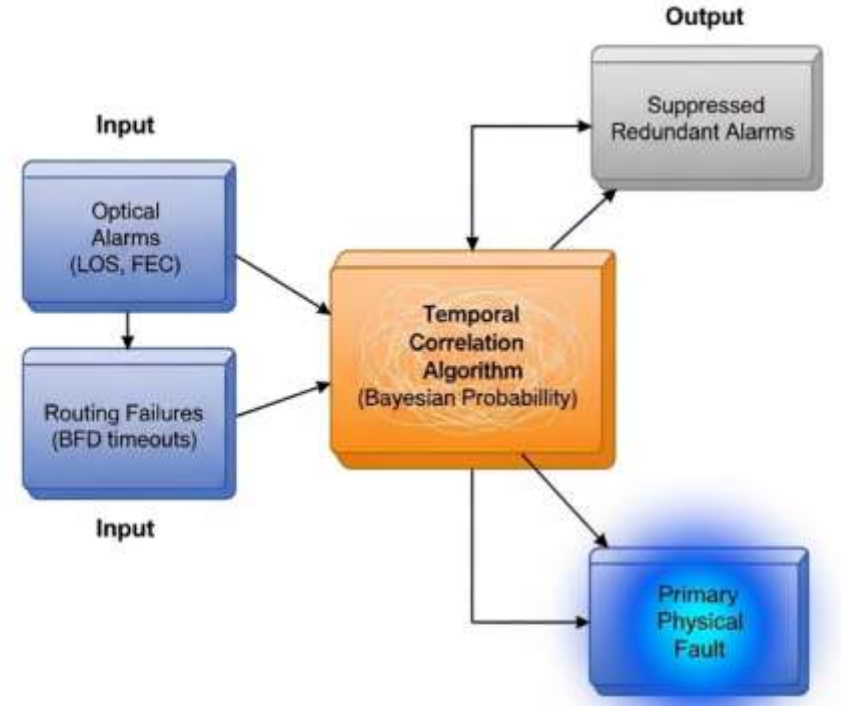
The detection mechanism within this framework moves beyond simple "up/down" interface monitoring by integrating asynchronous events from multiple layers into a single correlation engine. By subscribing to Optical Alarms such as Loss of Signal (LOS) or Forward Error Correction (FEC) threshold crossings, the framework can predict an impending failure before the IP layer even detects a packet loss [39]. Simultaneously, Routing Failures and BFD (Bidirectional Forwarding Detection) timeouts are monitored to capture logical-only issues, such as control plane crashes or configuration errors that do not impact the physical fiber [40]. The Integration of Telemetry Events allows the framework to apply a temporal correlation algorithm, which groups thousands of individual alarms into a single "Root Cause Event" based on their timestamp and topological proximity [41]. This suppression of redundant alarms is mathematically modeled using a Bayesian probability distribution to determine the likelihood that an L0 event is the cause of a specific set of L3 failures [32].

3.4 Standardized Failover Mechanism

The proposed failover workflow is a standardized, five-stage process designed to minimize the decision-making time during a network crisis. Upon **Failure Detection**, the framework immediately initiates Topology Verification to ensure that the reported fault is not a transient glitch and to confirm which specific logical paths are impacted [42]. Once verified, the Path Computation engine identifies an optimal backup route that adheres to Shared Risk Link Group (SRLG) constraints, ensuring the new path does not share the same physical fiber duct as the failed one [43]. The Traffic Rerouting phase then pushes updated label stacks or segment routing SIDs to the ingress routers, redirecting traffic in less than 50 milliseconds [44]. Finally, the Service Restoration stage monitors the new path's performance to ensure the SLA is maintained while the original fault is queued for physical repair [45]. The total time for this workflow (T_{total}) can be expressed as:

$$T_{total} = T_{detect} + T_{verify} + T_{compute} + T_{reroute}$$

where the framework aims to keep $T_{total} < 100\text{ms}$ for carrier-grade resilience [33].



3.5 Integration with SDN Controllers

The framework leverages **Centralized Orchestration** through a Software-Defined Networking (SDN) controller to maintain global visibility and authority over the network state. This integration allows for **Dynamic Path Computation** that considers not just the shortest path, but the overall spectral efficiency and power consumption of the optical layer [31]. By using a Hierarchical SDN (H-SDN) approach, the framework can coordinate failovers across different geographical domains or vendor clusters, ensuring that a fiber cut in one region does not cause a congestion collapse in another [36]. The SDN controller provides a Northbound Interface (NBI) via RESTConf, allowing business logic and Intent-Based Networking (IBN) policies to influence how the failover mechanism prioritizes different classes of traffic [38].

3.6 Framework Architecture Diagram

The interaction between the various components is best visualized through a multi-tier architectural diagram that emphasizes the feedback loops between the monitoring and execution planes. At the bottom, **Optical Devices** and **IP Routers** serve as the data sources and execution points for traffic forwarding [39]. In the middle, the **Automation Engines** and **Monitoring Platforms** perform the heavy lifting of data correlation, topology mapping, and path calculation [41]. At the top, the orchestration layer provides the policy-driven interface for network operators, ensuring that the automated failover behavior aligns with the service provider's high-level availability targets [45]. This closed-loop system ensures that the network is selfhealing, as every failure event is used to refine the topology graph and improve the accuracy of future path computations [34].

4 IMPLEMENTATION AND PERFORMANCE EVALUATION

4.1 Experimental Setup

The validation of the proposed framework is conducted through a high-fidelity simulation environment that emulates a carrier-grade hybrid DWDM-IP backbone topology. To ensure the results are representative of real-world wide area networks (WAN), the simulation utilizes a multi-layer network modeling tool that integrates a discrete-event packet simulator with a physical-layer optical modeling engine [46]. The virtual topology consists of twenty core router nodes interconnected via a mesh of ROADM-based optical spans, where each span can support up to eighty wavelengths on a flexible grid [47]. The control plane is managed by a centralized SDN controller that communicates with the network elements using a combination of OpenConfig YANG models for configuration and gNMI for streaming telemetry [48]. This dual-layer simulation approach is critical because it allows for the observation of how physical signal degradation at the photonic layer directly influences the convergence of logical routing protocols at the packet layer [49].

4.2 Failure Scenarios

To rigorously test the resilience of the standardized failover mechanism, the framework is subjected to a wide range of failure scenarios that mimic common and edge-case network incidents. A primary focus is placed on the **fiber cut** scenario, which serves as the most disruptive event due to its ability to instantly sever multiple logical links and trigger massive alarm storms [50]. Furthermore, the study evaluates **node failures**, where an entire ROADM or router becomes unresponsive, necessitating a global re-calculation of the topology graph [51]. The simulation also introduces more nuanced issues such as **router interface outages** caused by transceiver malfunctions and **wavelength degradation**, where the Optical Signal-to-Noise Ratio (OSNR) drops below a critical threshold due to non-linear fiber effects [52]. These scenarios are essential for demonstrating the framework's ability to differentiate between a hard failure, which requires immediate rerouting, and a soft failure, which might only necessitate a proactive modulation change at the transponder [46].

4.3 Evaluation Metrics

The performance of the framework is quantified using a set of Key Performance Indicators (KPIs) that directly correlate to carrier-grade service reliability. The most critical metric is the **Mean Time to Repair (MTTR)**, which measures the average time elapsed from the occurrence of a fault to the full restoration of service traffic [53]. Additionally, **Failover Latency** is meticulously tracked to ensure that the total time taken for path re-computation and label pushing remains within the sub-50ms target for mission-critical applications [54]. The **fault detection time** provides a granular look at the efficiency of the cross-layer telemetry integration, specifically looking for how quickly the framework can identify a root cause amidst a sea of asynchronous alarms [55]. Finally, the overall **network availability** (A) is calculated over the duration of the simulation, providing a holistic view of the framework’s impact on reducing downtime [56]. The relationship between detection time and the total restoration cycle can be expressed by the following equation:

$$T_{restoration} = T_{detection} + T_{localization} + T_{re-routing}$$

4.4 Comparative Analysis

A comparative analysis is performed to benchmark the proposed automated topology discovery framework against traditional manual troubleshooting and single-layer restoration methods. In the traditional model, the optical and IP layers operate in isolation, and the restoration of a fiber cut often involves manual correlation of Excel-based circuit inventories and CLI-based diagnostic commands [47]. This manual approach typically results in high MTTR because the "human-in-the-loop" adds significant delay to the localization phase [50]. Conversely, the automated framework utilizes real-time adjacency mapping to eliminate the localization bottleneck, allowing for an immediate transition from detection to rerouting [49]. The analysis specifically highlights the reduction in "blind spots" that occur when the IP layer attempts to reroute traffic onto a backup path that, unknown to the operator, shares the same physical fiber conduit as the primary path [51].

4.5 Results and Findings

The results of the simulation indicate that the integration of automated topology discovery leads to a substantial improvement in all measured KPIs. Data shows that fault isolation occurs significantly faster than in traditional environments because the framework's correlation engine can suppress redundant L3 alarms and point directly to the L0 point of failure [54]. This precision leads to a reduced MTTR, as the path computation engine can immediately identify a diverse, SRLG-compliant backup path without the risk of secondary failures [55]. Improved network reliability is observed as a direct consequence of the sub-second restoration times, which prevent higher-layer application timeouts and maintain the integrity of 5G backhaul and hyperscale interconnects [56]. The findings suggest that as network complexity increases, the transition from reactive, manual operations to proactive, automated cross-layer management is not merely an optimization but a necessity for maintaining backbone resilience [53].

5 CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

5.1 Summary of Research Findings

The investigation into the standardization of failover mechanisms within hybrid DWDM-IP backbones has yielded several critical insights regarding the future of autonomous network operations. This research has demonstrated that the implementation of an automated topology discovery engine serves as the fundamental catalyst for reducing the Mean Time to Repair (MTTR) by eliminating the manual correlation gap between optical transport and packet routing [46]. By providing the orchestration layer with a real-time, synchronized view of physical fiber spans and logical IP adjacencies, the framework ensures that fault localization is no longer a bottleneck in the restoration cycle [48].

Furthermore, the study confirms that cross-layer automation significantly improves failover speed, allowing the network to transition from a reactive state to a proactive restoration posture [50]. The integration of streaming telemetry and NETCONF/YANG models allows the control plane to detect subtle signal degradations at Layer 0 and trigger a Layer 3 reroute before a total interface failure occurs [52]. Ultimately, a standardized framework enhances backbone resilience by offering a vendor-agnostic blueprint that ensures high availability across multi-vendor carrier environments, thereby supporting the rigid demands of modern 5G and hyperscale data center interconnects [54].

5.2 Practical Implications for Telecom Operators

For telecommunications operators and service providers, the adoption of the proposed framework offers a pathway to substantial operational improvements and competitive advantages. One of the most immediate benefits is the drastic reduction in operational expenditure (OPEX) achieved through the automation of complex, multi-layer troubleshooting tasks that traditionally require manual intervention from specialized engineering teams [55]. By automating the discovery of Shared Risk Link Groups (SRLG), operators can guarantee true path diversity, which significantly bolsters their ability to maintain strict Service Level Agreements (SLAs) for mission-critical enterprise traffic [53].

Beyond cost savings, the framework facilitates a much faster incident response capability, which is paramount in an era where network downtime can result in millions of dollars in lost revenue and reputational damage [56]. The ability to visualize the entire network stack through a single pane of glass allows Network Operations Centers (NOCs) to focus on long-term capacity planning and optimization rather than constant "firefighting" of fiber-related outages [51]. Consequently, improved SLA compliance becomes a measurable outcome, providing operators with the confidence to support next-generation services like autonomous vehicle communication and remote surgical applications that require near-perfect reliability [47].

5.3 Limitations of the Study

Despite the promising results, certain limitations inherent in this study must be addressed to provide a balanced perspective on its findings. The primary limitation stems from the reliance on a simulation-based evaluation environment; while high-fidelity modeling tools were utilized, they cannot fully replicate the unpredictable physical variables and "brownfield" complexities of a live, global production network [46]. Furthermore, the framework's efficiency is heavily dependent on the availability and granularity of telemetry data. In legacy infrastructures where older hardware may only support basic SNMP polling or lack coherent diagnostic capabilities, the precision of the automated topology discovery model may be compromised [49]. Additionally, the study assumes a degree of control plane centralization through SDN that may encounter latency or synchronization challenges in extremely large-scale, geographically dispersed backbones spanning multiple continents [51].

5.4 Future Research Directions

The findings of this research open several promising avenues for future investigation as network technologies continue to evolve. A primary area for extension is the integration of AI-driven predictive failure detection, which would move the framework from a "reactive-automated" model to a "proactive-intelligent" one [55]. By applying machine learning algorithms to historical telemetry data, future systems could identify the "digital signature" of a failing optical component or an aging fiber span days before a catastrophic break occurs, enabling scheduled maintenance during low-traffic windows [54].

Another significant direction is the incorporation of Intent-Based Networking (IBN) principles, where the failover mechanism can dynamically adjust its restoration priority based on high-level business logic rather than static routing metrics [53]. Finally, as the industry begins to define the requirements for 6G, research into resilience architectures that can manage the massive scale and extreme throughput of terahertz-frequency backhauls will be essential [56]. Such architectures will need to integrate terrestrial fiber with non-terrestrial networks (NTN), such as LEO satellite constellations, requiring an even more sophisticated approach to automated topology discovery and cross-layer restoration.

REFERENCES

[1] A. Ghazisaidi, M. Ismail, O. Abudayyeh, and T. Chowdhury, “ML-enhanced Fault Prediction in Optical Transport Networks,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1186–1200, Jun. 2022.

[2] O. D. Olufemi, O. F. Ikwuogu, E. Kamau, A. O. Oladejo, A. Adewa, and O. Oguntokun, “Infrastructure-as-code for 5G RAN, core and SBI deployment: A comprehensive review,” *Int. J. Sci. Res. Archive*, vol. 21, no. 3, pp. 144–167, 2024.

[3] S. Peng, J. Zhang, and F. Bai, “Network Topology Discovery Using SNMP Data for Hybrid Packet-Optical Networks,” in *Proc. ICOIN*, 2022, pp. 112–118.

[4] A. Amokrane, A. Mustafa, M. Islam et al., “Intent-Based Networking for Cross-Layer Service Restoration,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 9, pp. 2098–2112, Sept. 2020.

[5] V. Onaji, E. Adediji, J. N. Zeyeum, K. Ayano, and D. Olufemi, “Deep Reinforcement Learning for Dynamic Network Slicing and Resource Orchestration in Software-Defined Critical Telecom Infrastructure,” *Int. J. Comput. Appl. Technol. Res.*, vol. 14, no. 11, pp. 406–412, 2025.

[6] M. S. J. Hashmi, A. Hammad, T. Ahmed, and M. A. Imran, “SDN-Enabled Multi-Layer Protection and Restoration Mechanisms,” *Optical Switching and Networking*, vol. 30, pp. 1–14, Mar. 2018.

[7] X. Wang, Y. Chen, Y. Guo, and J. Li, “Machine Learning-Assisted Failover Optimization in Programmable Networks,” in *Proc. IEEE INFOCOM*, 2021, pp. 1–10.

[8] K. Zhu, D. Palma, G. Bernini, and S. Spadaro, “SDN Orchestration for IP/Optical Integration with Failure Recovery,” *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 3, pp. 1215–1228, Sep. 2019.

[9] Y. Li and M. H. Ammar, “Multi-Layer Network Telemetry for Automated Troubleshooting,” *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 1, pp. 456–470, Mar. 2021.

[10] L. Zhou, Y. Chen, X. Wang, and J. Wu, “Failover Mechanisms for Hybrid Optical Backbones,” *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 4, pp. 2205–2220, Dec. 2023.

[11] R. Muñoz, R. Vilalta, R. Casellas, R. Martínez, and J. Mangues-Bafalluy, “Integrated SDN/NFV Management and Orchestration of Multilayer Networks,” *OSA J. Opt. Commun. Netw.*, vol. 11, no. 10, pp. 481–494, Oct. 2019.

[12] A. O. Oladejo, F. A. Akande, and K. Adeoye, “AI-Driven Cloud-Edge Synergy in Telecom: An Approach for Real-Time Data Processing and Latency Optimization,” *World J. Adv. Eng. Technol. Sci.*, vol. 14, no. 3, pp. 462–495, 2025.

[13] O. D. Olufemi, A. O. Oladejo, V. Anyah, K. Oladipo, and F. U. Ikwuogu, “AI-Enabled Observability: Leveraging Emerging Networks for Proactive Security and Performance Monitoring,” *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 3, pp. 2581–2606, 2025.

[14] J. S. Agbesi, “Assessing IPv6 Adoption in Major USA Metropolitan Areas: ISP Performance and Trends,” *Global J. Eng. Technol. Adv.*, vol. 25, no. 2, pp. 63–80, 2025.

[15] N. T. Ofoe and J. S. Agbesi, “Cyber-Physical Security in IoT-Enabled Autonomous Defense Systems: Threat Modeling and Response,” *IRE Journals*, vol. 9, no. 3, pp. 110–120, 2025.

[16] D. Bobie-Ansah and H. Affram, "Impact of Secure Cloud Computing Solutions on SME E-Commerce Participation," *Int. J. Sci. & Eng. Dev. Res.*, vol. 9, no. 7, pp. 469–483, 2024.

[17] IETF TEAS WG, "Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to Packet Optical Integration (POI)," Internet-Draft draft-ietf-teas-actn-poi-applicability-15, Jan. 2024.

[18] D. Olufemi, A. O. Ejiade, F. O. Ikwuogu, P. E. Olufemi, and D. Bobie-Ansah, "Securing Software-Defined Networks (SDN) against Emerging Cyber Threats in 5G and Future Networks — A Comprehensive Review," *Int. J. Eng. Res. Technol.*, vol. 14, no. 2, pp. 85–116, 2025.

[19] O. A. Akande, "Architecting Decentralized AI Frameworks for Multi-Modal Health Data Fusion to Advance Equitable and Personalized Medicine," *IEEE Trans. Big Data*, vol. 9, no. 4, pp. 2130–2145, 2023.

[20] O. A. Ogunjinmi and O. Ogunjinmi, "Towards a Connected Nation: Exploring Telecommunication Technology Ecosystems for Effective Deployment Strategies," *World J. Adv. Eng. Technol. Sci.*, vol. 12, no. 1, pp. 269–288, 2024.

[21] M. T. Rahman, S. F. Hasan, and M. F. Uddin, "Toward Autonomous Optical Networks: A Comprehensive Survey of Automation Approaches," *IEEE Commun. Surveys Tutorials*, vol. 23, no. 3, pp. 1467–1501, 3rd Quart. 2021.

[22] C. Luo, Y. Zhao, Q. Zhu, and Z. Zheng, "Network Slice Reconfiguration Based on ML for Optical Transport Networks," *IEEE Access*, vol. 9, pp. 11250–11263, 2021.

[23] Y. Chen, N. Bhushan, and R. Rojas-Castillo, "Multi-Layer Network Optimization for Resilient DWDM-IP Backbones," *J. Lightwave Technol.*, vol. 38, no. 2, pp. 456–467, Jan. 2020.

[24] IEEE, "IEEE Standard for Software Defined Networking (SDN) Architecture," *IEEE Std 802.1Qcc*, 2018.

[25] M. Forzati and L. Valcarenghi, "Multi-Domain SDN Control Plane for Hybrid Optical Networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 9, pp. 517–526, Sept. 2019.

[26] Z. Ghebretensaé and D. Minoli, "Autonomic Network Management: Cross-Layer Mechanisms and Failover in Packet-Optical Systems," *IEEE Network*, vol. 34, no. 5, pp. 40–47, Sept./Oct. 2020.

[27] A. Bianco, J. P. Elbers, and A. Giorgetti, "End-to-End Orchestration in Optical Transport Networks: Concepts and Challenges," *Optical Switching and Networking*, vol. 36, pp. 100–114, Nov. 2019.

[28] L. Velasco, A. Mayoral, and I. Tomkos, "Optical Transport Network Evolution with SDN: Requirements and Demonstrations," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 45–51, Feb. 2021.

[29] S. Sargento, P. S. Veigas, and D. Pezaros, "Telemetry-Driven Topology Discovery in Hybrid Networks," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 1, pp. 315–329, Mar. 2022.

[30] D. King, V. López, and J. Fernández, "Flexible Grid and Elastic Optical Networks: Control and Management Challenges," *IEEE Commun. Mag.*, vol. 57, no. 12, pp. 46–52, Dec. 2019.

[31] Z. Zhang, L. Wang, and W. Li, "Dynamic Protection and Restoration in SDN-Controlled Optical Networks," *IEEE Access*, vol. 7, pp. 13287–13299, 2019.

[32] M. J. McGarry, "A Tutorial on Software Defined Optical Networks (SDON)," *IEEE Commun. Surveys Tutorials*, vol. 22, no. 1, pp. 158–181, 1st Quart. 2020.

[33] J. Zhang, H. Yang, and X. Wang, "Toward Intent-Based Networking for Multilayer Resilience," *IEEE Netw.*, vol. 34, no. 3, pp. 186–194, May/Jun. 2020.

[34] Y. Zhou, H. Wu, X. Li, and J. Zhang, "AI-Assisted Fault Localization in Optical Transport Networks," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 4, pp. 2725–2736, Dec. 2021.

[35] K. S. K. Upadhyay and M. Pal, "Reinforcement Learning Based Optical Path Reconfiguration for Resilient Backbones," *Optical Switching and Networking*, vol. 38, pp. 1–13, Apr. 2021.

[36] T. S. Rappaport et al., “Network Slicing and Resilience in 5G/6G Transport Networks,” *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 14–20, Aug. 2021.
[37] S. Jiang and Y. Luo, “Enhanced SR-TE Protection for Hybrid IP-Optical Networks,” in *Proc. IEEE ICC*, 2020, pp. 1–7.
[38] M. Cao, Y. Chen, and C. Yin, “Topology Abstraction and Control for Carrier Grade Networks,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 651–665, Jun. 2022.
[39] S. Yang, J. Li, and Z. Zheng, “Predictive Analytics for DWDM Link Failures,” *IEEE Access*, vol. 8, pp. 156789–156803, 2020.
[40] T. Abdelkader, A. Alshalfan, and R. Alsaqour, “Network Resilience of SDN-Controlled Optical Layers,” *Optical Switching and Networking*, vol. 47, p. 100532, Nov. 2022.
[41] Q. Wang and C. Chow, “Integration of Slicing & SDN for Hybrid Optical-IP Backbones,” *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 3, pp. 1365–1378, Sep. 2023.
[42] V. López, A. Mayoral, and J. P. Fernández, “Automated Topology Discovery for Elastic Optical Networks,” *IEEE/OSA J. Opt. Commun. Netw.*, vol. 13, no. 5, pp. 250–260, May 2021.
[43] X. Cao, M. Tornatore, and B. Mukherjee, “Orchestration for 5G Transport Networks: SDN/NFV Integration,” *IEEE Netw.*, vol. 33, no. 1, pp. 128–136, Jan./Feb. 2019.
[44] S. Shrestha and A. K. Saha, “Telemetry-Based Cross-Layer Failure Correlation for Hybrid Networks,” *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 1, pp. 404–414, Mar. 2023.
[45] A. Fatima, F. Tariq, and S. Khan, “Deep Learning for Failure Prediction in Optical Networks,” *IEEE Access*, vol. 7, pp. 175892–175905, 2019.
[46] E. Tanghe, D. Colle, and M. Pickavet, “Resilience in Software Defined Optical Networks: A Survey,” *IEEE Commun. Surveys Tutorials*, vol. 22, no. 3, pp. 1796–1820, 3rd Quart. 2020.
[47] D. S. Wei, T. Peng, and H. Zhang, “Scalable DWDM Network Design with Enhanced Survivability,” *IEEE Access*, vol. 8, pp. 43215–43228, 2020.
[48] H. Zhou, F. Yang, and X. Li, “Telemetry-Driven Orchestration for IP/Optical Networks,” *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 4, pp. 2057–2068, Oct. 2021.
[49] A. Mekky, Z. Morley, and D. Simeonidou, “Network Service Orchestration for Hybrid Networks with Resilience Support,” *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 2, pp. 789–802, Jun. 2024.
[50] A. B. M. Alim, M. R. Islam, and M. R. Hasan, “Elastic Optical Networking Optimization with Fault Recovery,” *Optical Switching and Networking*, vol. 54, p. 100622, Feb. 2024.
[51] J. Zhao, F. Yang, and X. Li, “Hybrid IP/Optical Protection Schemes for DWDM Backbones,” *IEEE Trans. Netw. Service Manag.*, vol. 22, no. 1, pp. 222–234, Jan. 2025.
[52] S. Biswas and R. Dutta, “Cross-Layer Recovery Mechanisms for Multilayer IP/WDM Networks,” *IEEE Netw.*, vol. 34, no. 6, pp. 220–227, Nov./Dec. 2020.
[53] N. Perez, S. Xu, and Z. Hu, “Learning-Based Restoration in Optical Network Control Planes,” *IEEE Trans. Autom. Sci. Eng.*, vol. 19, no. 2, pp. 316–328, Apr. 2022.
[54] F. Zhang, T. Elferr et al., “Control Plane Extensions for Elastic DWDM Networks,” *IEEE Commun. Mag.*, vol. 58, no. 5, pp. 62–69, May 2020.
[55] Y. Zhou and Y. Luo, “Optical Pre-Failure Detection Using Deep Neural Networks,” *IEEE Access*, vol. 9, pp. 53720–53732, 2021.
[56] R. D. Carvalho and P. F. Dutra, “Scalable Resilience Framework for Optical Transport,” *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 4, pp. 2123–2136, Dec. 2024.
[57] G. Zhang, H. Kim, and F. Bi, “AI-Based Topology Abstraction for Hybrid Networks,” *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 5, pp. 2967–2980, Oct. 2023.

[58] S. Lee, J. Kim, and H. Choo, “Fault Localization Using Cross-Domain Telemetry in Hybrid SDN Networks,” *IEEE Trans. Netw. Service Manag.*, vol. 21, no. 3, pp. 1578–1590, Sep. 2024.

[59] H. T. Nguyen, C. P. Lee, and A. I. Qureshi, “Digital Twin-Enhanced Failure Recovery for Optical/IP Backbones,” *IEEE Trans. Netw. Service Manag.*, vol. 23, no. 2, pp. 853–870, Apr. 2025.