

# Transforming Enterprise Office Networks with EVPN-VXLAN: A BGP-Based Approach to Layer 2 Elimination

(Authors Details)

**Brandon Warren**

Global Architect, Houston Packard Enterprise

Email: [bwarren@eagle.org](mailto:bwarren@eagle.org)

## Abstract

As new demands for scalability, flexibility, cloud integration, and operational efficiency arise in enterprise office networks, there is a need for significant transformation. While using traditional Layer 2 spanning tree protocols may give some enterprises lower traffic utilization, slower convergence, higher broadcast overheads, and limited scalability, it can also add complexity when it comes to managing them. Traditional Layer 2 spanning tree protocols can also limit an enterprise's traffic utilization, convergence rate, broadcast overheads, and scalability in a large-scale network, while also increasing management complexity. In this study, the authors present an enterprise network modernization approach that removes legacy L2 dependencies by implementing Ethernet VPN (EVPN) and Virtual Extensible LAN (VXLAN) technologies in combination with a Border Gateway Protocol (BGP)-based control plane.

The proposed architecture will bring EVPN-VXLAN over-layer technology to the enterprise office infrastructures to meet the needs of scalable segmentation, optimized traffic forwarding, enhanced redundancy, and rapid converging. The model enhances network resiliency, operational management, and seamlessly integrates into SDN and cloud networking environments, all while replacing legacy Layer 2 mechanisms with a BGP-based approach. The study also considers the architectural benefits of EVPN-VXLAN in the areas of throughput, fault tolerance, scalability, and broadcast traffic reduction when compared to traditional enterprise networking solutions.

Furthermore, the study sheds light on the importance of programmable networking, automation, and intelligent monitoring for enhancing enterprise network performance and adaptability. The results prove that EVPN-VXLAN is a powerful, future-proof architecture that can enable enterprise digital transformation projects while solving the problems of traditional Layer 2 architectures.

**Keywords:** EVPN-VXLAN, BGP, Enterprise Networks, Layer 2 Elimination, Network Transformation, VXLAN Overlay, Digital Transformation, Software-Defined Networking, Enterprise Architecture, Network Scalability.

**DOI:** 10.21590/ijtmh.07.4.07

## **I. Introduction**

Enterprise office networks have undergone significant architectural change over a short period of time because of rapidly increasing cloud computing, virtualization, mobility services, distributed applications and digitally connected business environments. Traditional enterprise networking models grew up around Layer 2 Ethernet domains and spanning tree protocols; they were designed to support relatively static infrastructures that have relatively modest scalability requirements. In today's enterprise environment, however, we require highly scalable, flexible, resilient and programmable network infrastructures to support dynamically changing workloads and geographically distributed operations (Hanna, 2010; Schwertner, 2017).

STP mechanisms are used extensively in conventional Layer 2 enterprise architectures to prevent loops and offer redundancy management. While STP is useful for providing operational stability, it also has several drawbacks such as: Redundant paths are blocked off, Bandwidth can be wasted, Topology changes take a long time to converge, and Broadcast propagation is too high. In large enterprise office environments, these limitations become significant if the environment's operational requirements are high availability, quick failover and mobility of workloads (Nadaf et al., 2012). With organizations still working on digital transformation projects, enterprise network infrastructures need to go beyond legacy Layer 2 designs that prove limiting in their ability to deliver automation, scalability, and cloud-based service delivery (Gong et al., 2020).

Virtual Extensible LAN (VXLAN) and Ethernet Virtual Private Network (EVPN) technologies have greatly revolutionized enterprise network designs by introducing scalable overlay networking and contemporary control plane solutions. VXLAN is an implementation of Layer 2 overlay network on top of Layer 3 underlay network and it helps to overcome the scalability limitation of VLANs, while providing multi-tenant environments and enabling workload mobility. EVPN extends VXLAN by introducing a standards-based control plane mechanism for efficient advertisement of MAC and IP routes, host reachability, and dynamic endpoint learning, via the Border Gateway Protocol (BGP) (Krattiger et al., 2017). This pairing creates a network architecture that is very scalable and resilient, and that can do without traditional spanning tree protocols.

Through the use of Equal-Cost Multi-Path (ECMP) forwarding, distributed gateway functionality, optimized traffic engineering, and rapid convergence mechanisms, BGP-based EVPN-VXLAN architectures allow the enterprise office network to run using these functions. EVPN uses control-plane learning methods to minimize the traffic propagation and to make the operation more efficient unlike conventional Layer 2 networks that rely on broadcast and flood-based learning. Moreover, BGP can be used in enterprise fabrics to improve policy-based routing control, segmentation and network scalability in campus and branch office networks (Pucci & Casoni, 2020).

Network programmatization has been further driven by the growing adoption of software-defined networking (SDN), automation platforms and intelligent network management systems. Centralized orchestration and dynamic service provisioning in large-scale networks have been proven to be

achievable in SDN based Layer 2 and IP services (Ventre et al., 2017). Furthermore, the contribution of AI and machine learning technologies in enterprise network operations has been growing and is used to optimize traffic, detect faults and make autonomous decision-making (Gupta et al., 2018). All of these emerge as a confirmation of the need for modern architectures that enable adaptive and intelligent enterprise operations.

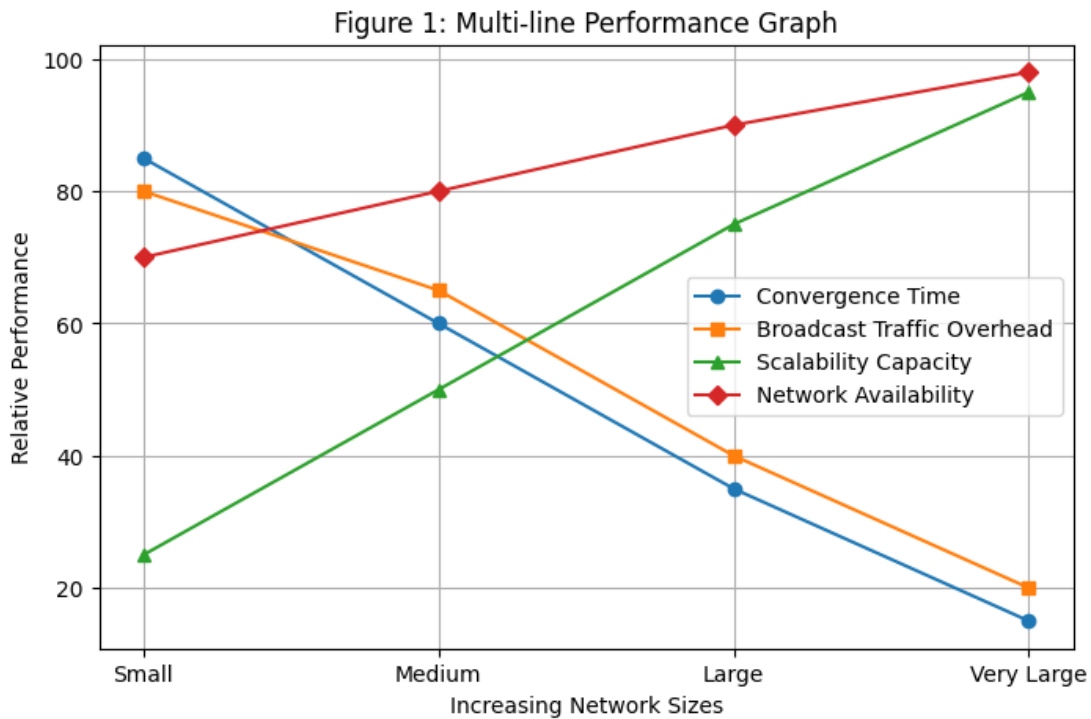
While EVPN-VXLAN deployments offer several benefits, there are some operational and security issues that should be considered. If not well protected and monitored, BGP routing infrastructures can have vulnerabilities from route manipulation, misconfigurations, and routing instability (Lychev et al., 2013). Research into public BGP environments have also reported spurious route propagation and routing inconsistencies which can affect network reliability (Luckie, 2014). Therefore, it is important to have proper monitoring frameworks, route validation mechanisms, and visibility based on telemetry for maintaining a stable EVPN-VXLAN enterprise fabric (Pucci & Casoni, 2020).

In this research, we examine how enterprise office networks are changing to become more virtualized through EVPN-VXLAN architectures leveraging a BGP-based control plane to remove legacy Layer 2 dependency. It's primarily a study of architectural modernization, operational efficiencies, scalability enhancements, traffic optimization and resiliency improvements in enterprise environments. The proposed approach demonstrates how EVPN-VXLAN can provide a future-ready networking framework capable of supporting modern enterprise digital transformation initiatives while addressing the limitations associated with conventional Layer 2 network infrastructures.

**Table 1. Comparative Analysis of Traditional Enterprise Networks and EVPN-VXLAN Architectures**

Network Parameter	Traditional Layer 2 Architecture	EVPN-VXLAN Architecture
Control Plane	Spanning Tree Protocol	BGP EVPN
Network Scalability	Limited VLAN Scale	Large VXLAN Scale
Traffic Utilization	Blocked Redundant Links	ECMP Active Paths
Convergence Speed	Slow	Rapid
Broadcast Dependency	High	Reduced
Fault Tolerance	Moderate	High
Segmentation Capability	VLAN-Based	VXLAN Overlay
Automation Support	Limited	Extensive

Multi-Tenancy	Restricted	Fully Supported
Cloud Integration	Complex	Simplified
Monitoring Visibility	Conventional SNMP	Telemetry and BMP
Operational Flexibility	Static	Dynamic



**Figure 1:** EVPN-VXLAN architectures demonstrate improved scalability, lower broadcast overhead, faster convergence, and higher network availability compared to traditional Layer 2 enterprise networks as network size increases.

## II. Related Work and Literature Review

With rising requirements for scalability, virtualization, cloud integration and operational agility, enterprise networking has undergone a remarkable transformation. Early enterprise office networks were mostly based on hierarchical Layer 2 Switching with spanning tree protocols (STP), VLAN segmentation and static operational processes. While these methods made it easy to connect enterprises early on, they also added some drawbacks such as inefficient path utilization, too many

broadcast domains, slow convergence, and limited scalability in a large-scale network. Digital transformation programs have created a demand for more programmable, resilient and intelligent enterprise networking infrastructures (Hanna, 2010; Schwertner, 2017).

Early enterprise transformation studies focused on the need to optimize the network and upgrade its infrastructure to meet the organization's increasing demand. The methods that were proposed by Nadaf et al. (2012) are enterprise transformation methodologies that provide the benefits of operational efficiency, scalability of networks and optimization of services. They were responsible for the introduction of the wide-spread need for businesses to move away from traditional network architectures to more flexible and service-based solutions. Likewise, Maan (2012) explained enterprise transformation by mobility and interconnected communication architectures, and showed that the modern enterprise services are increasingly reliant on flexible networking environments that can support distributed applications and real-time communication.

In addition, the increasing uptake of cloud computing and virtualization drove the demand for scalable enterprise network architectures. The need for scalable enterprise network architectures was further increased by the rapid growth of cloud computing and virtualisation. Chang et al. (2010) stated that enterprise cloud transformation raised three new networking issues: traffic engineering, workload mobility, and dynamic resource allocation. Traditional Layer 2 solutions found themselves unable to meet these needs efficiently as they were limited in their ability to scale and be flexible with their operations. Overlay-based networking models started to become an option for enterprises in modern infrastructures as organisations spread their offices around and adopted Cloud integration.

The VXLAN technology was introduced to address the scalability issues that traditional VLAN architectures have. VXLAN, according to Krattiger et al. (2017), is a network virtualization technique that provides an overlay mechanism to extend existing Layer 2 connectivity across a Layer 3 network using encapsulated overlays. Their work demonstrated that VXLAN, when integrated with EVPN as the control plane, enables highly scalable and efficient fabric architectures that support multi-tenancy, workload mobility, and simplified operational management. EVPN-VXLAN architectures provide significant improvements over conventional Layer 2 environments by replacing flood-and-learn mechanisms with control-plane learning through BGP advertisements. This approach minimizes broadcast traffic, improves convergence, and enhances traffic optimization using Equal Cost Multi-Path (ECMP) forwarding.

The adoption of BGP as the control-plane protocol for EVPN fabrics has been widely studied due to its scalability and policy control capabilities. Lychev et al. (2013) examined BGP security challenges during partial deployment scenarios and highlighted the importance of secure route advertisement mechanisms in large-scale distributed networks. Their findings emphasized that although BGP offers considerable flexibility and scalability, improper deployment or insufficient validation mechanisms may expose enterprise environments to route manipulation and instability risks. Similarly, Luckie (2014) analyzed spurious routing behavior in public BGP datasets and

demonstrated how inaccurate route propagation can impact network stability and operational visibility. These studies underline the necessity of implementing robust route filtering, validation, and monitoring frameworks within EVPN-VXLAN deployments.

Further research on BGP-based networking evaluated performance characteristics in IPv6 and service provider environments. Al-Mehdhar (2013) investigated IPv6 BGP-based solutions and analyzed their effectiveness in handling malicious traffic scenarios and routing policy enforcement. The study demonstrated that BGP-driven architectures can achieve improved flexibility and policy-based traffic control when compared to static routing approaches. These findings are relevant to EVPN-VXLAN enterprise fabrics because modern office networks increasingly require scalable routing frameworks capable of supporting hybrid cloud connectivity, distributed branches, and security-driven segmentation policies.

Software-Defined Networking (SDN) also contributed significantly to the evolution of enterprise network architectures. Ventre et al. (2017) proposed SDN-based IP and Layer 2 service integration using open networking operating systems within large-scale service provider networks. Their research demonstrated how centralized programmability and automation improve service orchestration, network abstraction, and operational efficiency. The integration of SDN principles with EVPN-VXLAN fabrics provides enterprises with dynamic traffic engineering, centralized policy management, and improved visibility across distributed office infrastructures. Ventre-GARR et al. further reinforced the role of SDN-enabled Layer 2 virtualization in improving service flexibility and reducing dependency on traditional network control mechanisms.

Network visibility and operational monitoring have become increasingly important in EVPN-VXLAN deployments due to the complexity of overlay-underlay interactions. Pucci and Casoni (2020) proposed monitoring techniques for EVPN-VXLAN fabrics using the BGP Monitoring Protocol (BMP). Their work demonstrated that real-time telemetry and route monitoring significantly improve operational awareness and fault diagnosis in BGP-driven fabrics. Enterprise environments deploying EVPN-VXLAN architectures require advanced monitoring frameworks to maintain visibility across distributed overlays, detect route inconsistencies, and ensure network stability. The incorporation of telemetry-driven monitoring mechanisms therefore plays a critical role in maintaining reliable enterprise network operations.

The increasing adoption of artificial intelligence and automation technologies has further transformed enterprise networking strategies. Gupta et al. (2018) explored the application of artificial intelligence in autonomous enterprise networks and emphasized the benefits of intelligent automation in traffic analysis, anomaly detection, predictive maintenance, and policy optimization. AI-driven networking introduces adaptive operational capabilities that complement EVPN-VXLAN infrastructures by enabling automated fault remediation, dynamic traffic

optimization, and intelligent resource allocation. These capabilities are essential for modern enterprise office environments that require high availability, scalability, and minimal operational overhead.

Digital transformation research also highlights the broader organizational impact of enterprise network modernization. Gong et al. (2020) examined enterprise architecture flexibility within digital transformation frameworks and emphasized that adaptable network infrastructures are critical for supporting evolving business processes and distributed services. Fraser and Dutta (2010) further discussed how interconnected digital ecosystems and collaborative technologies influence enterprise operational models, thereby increasing demand for scalable and resilient networking infrastructures. The transition toward EVPN-VXLAN fabrics aligns with these digital transformation objectives by enabling agile service delivery, improved connectivity, and enhanced operational efficiency across enterprise office networks.

Overall, the reviewed literature demonstrates a clear transition from traditional Layer 2 enterprise networking models toward scalable, programmable, and BGP-driven architectures. Existing studies consistently identify limitations in conventional spanning tree-based environments while emphasizing the operational advantages of EVPN-VXLAN overlays, SDN integration, telemetry-driven monitoring, and intelligent automation. However, despite extensive research on data center EVPN deployments, fewer studies focus specifically on enterprise office network transformation using EVPN-VXLAN architectures. This creates a research gap concerning the application of BGP-based Layer 2 elimination strategies in distributed enterprise office environments, particularly in relation to operational efficiency, scalability, and network resiliency.

**Table 2. Summary of Related Literature on Enterprise Network Transformation and EVPN-VXLAN**

Author(s)	Research Focus	Key Contribution	Relevance to EVPN-VXLAN Enterprise Networks
Hanna (2010)	Enterprise transformation	Digital infrastructure modernization	Supports enterprise network evolution
Chang et al. (2010)	Enterprise cloud services	Cloud-driven infrastructure transformation	Highlights need for scalable overlays
Nadaf et al. (2012)	Enterprise network optimization	Network transformation methodologies	Foundation for enterprise modernization

Maan (2012)	Connected enterprise systems	Mobility-driven enterprise networking	Supports distributed office connectivity
Lychev et al. (2013)	BGP security	Security analysis of BGP deployments	Relevant to EVPN control-plane security
Al-Mehdhar (2013)	IPv6 BGP performance	Policy-based routing evaluation	Demonstrates scalability of BGP frameworks
Luckie (2014)	BGP route anomalies	Analysis of routing instability	Highlights monitoring importance
Krattiger et al. (2017)	VXLAN BGP EVPN	EVPN-VXLAN fabric architecture	Core foundation for modern overlays
Ventre et al. (2017)	SDN Layer 2 services	Programmable networking integration	Supports automation and virtualization
Schwertner (2017)	Digital business transformation	Business modernization through technology	Supports enterprise infrastructure evolution
Gupta et al. (2018)	AI in enterprise networking	Intelligent network automation	Enhances EVPN operational efficiency
Pucci & Casoni (2020)	EVPN monitoring	BMP-based EVPN observability	Improves network telemetry and visibility
Gong et al. (2020)	Enterprise architecture flexibility	Digital transformation analysis	Supports scalable enterprise fabrics

### **III. Enterprise Network Architecture Transformation**

Enterprise office environments have evolved from relatively static communication infrastructures into highly dynamic digital platforms supporting cloud services, virtualization, mobility, collaboration systems, and distributed applications. Traditional enterprise networks built upon Layer 2 Ethernet domains and spanning tree protocols increasingly struggle to meet the operational requirements of scalability, resiliency, agility, and traffic optimization demanded by modern organizations. As enterprise digital transformation accelerates, network infrastructures are required to support flexible service delivery, rapid provisioning, and seamless integration with cloud-native environments (Hanna, 2010; Schwertner, 2017).

Conventional Layer 2 enterprise architectures rely heavily on VLAN segmentation and spanning tree mechanisms to prevent loops within switched environments. Although these mechanisms have historically provided operational stability, they introduce significant inefficiencies in large-scale enterprise deployments. Spanning Tree Protocol (STP) blocks redundant links to avoid loops, resulting in underutilization of available bandwidth and slower convergence during network failures. In addition, increasing VLAN complexity across multiple office locations complicates management and limits scalability (Nadaf et al., 2012).

The emergence of EVPN-VXLAN introduces a modern overlay-based architecture capable of eliminating many of the operational limitations associated with legacy Layer 2 networking. VXLAN provides network virtualization through Layer 2 overlay tunnels across Layer 3 IP underlays, while EVPN utilizes BGP as the control-plane mechanism for endpoint discovery, MAC address advertisement, and routing information exchange (Krattiger et al., 2017). This architectural model enables enterprises to transition from hardware-dependent Layer 2 domains toward scalable and programmable network fabrics.

### **3.1 Legacy Enterprise Network Limitations**

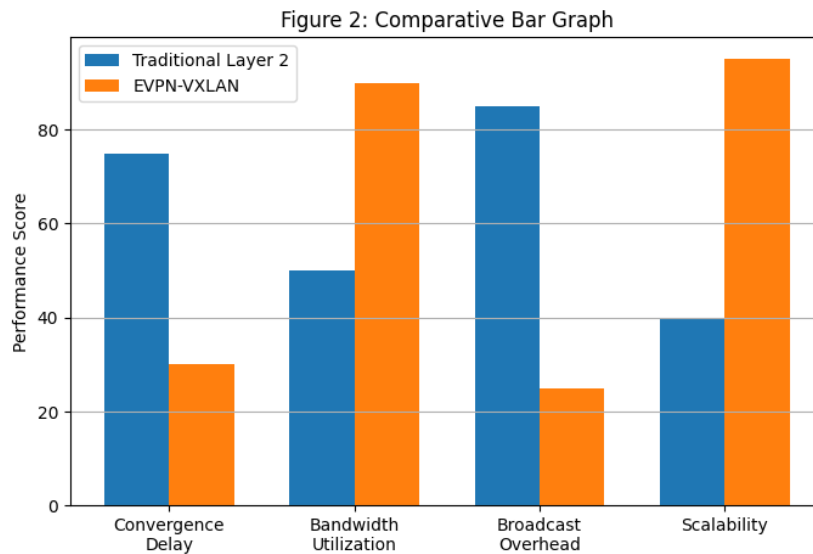
Legacy office network infrastructures typically operate using hierarchical access, distribution, and core layers interconnected through VLAN-based Ethernet switching. While this design simplifies segmentation within smaller deployments, several operational challenges emerge as enterprise environments expand. These include:

- Excessive broadcast and unknown unicast flooding
- Slow convergence during topology changes
- Limited VLAN scalability
- Complex inter-site Layer 2 extension
- Increased operational overhead in large office campuses
- Inability to efficiently utilize redundant network paths

Furthermore, the rapid adoption of cloud services and mobility-driven applications has increased east-west traffic patterns within enterprise environments. Traditional architectures optimized primarily for north-south traffic flows become inefficient under these conditions (Chang et al., 2010).

**Table 3. Limitations of Traditional Enterprise Layer 2 Architectures**

Network Aspect	Traditional Layer 2 Architecture	Operational Impact
Loop Prevention	Spanning Tree Protocol	Blocked redundant links
Convergence Speed	Slow	Service interruption
VLAN Scalability	Limited	Complex segmentation
Traffic Utilization	Inefficient	Reduced bandwidth usage
Broadcast Management	High broadcast domains	Increased overhead
Multi-site Extension	Difficult	Complex configuration



**Figure 2:** The bar graph highlights that EVPN-VXLAN architectures provide better bandwidth utilization and scalability while significantly reducing convergence delay and broadcast overhead relative to traditional Layer 2 networks.

### 3.2 Transition Toward EVPN-VXLAN Architecture

To address the limitations of traditional enterprise designs, organizations increasingly adopt EVPN-VXLAN fabrics based on BGP-enabled control planes. In this model, the enterprise network is divided into two primary components:

1. IP Underlay Network
2. VXLAN Overlay Network

The IP underlay provides reliable Layer 3 connectivity between network devices using dynamic routing protocols such as BGP. Above this foundation, VXLAN establishes logical Layer 2 overlays that enable scalable tenant segmentation independent of physical topology (Krattiger et al., 2017).

Unlike traditional Ethernet switching, EVPN-VXLAN eliminates the dependency on spanning tree protocols by leveraging Equal-Cost Multi-Path (ECMP) forwarding. ECMP enables all available paths to actively forward traffic, significantly improving bandwidth utilization and fault tolerance. The use of BGP as the control plane further enhances scalability through distributed route learning and efficient endpoint advertisement mechanisms (Pucci & Casoni, 2020).

The transformation toward EVPN-VXLAN also simplifies enterprise mobility and workload migration across distributed office locations. Since VXLAN overlays abstract network segmentation from physical infrastructure, services can be dynamically extended without major topology modifications. This flexibility aligns closely with modern enterprise transformation strategies emphasizing agility, virtualization, and cloud readiness (Gong et al., 2020).

### **3.3 BGP-Based Control Plane Integration**

Border Gateway Protocol serves as the foundational control-plane mechanism within EVPN-VXLAN architectures. Through EVPN route advertisements, BGP distributes MAC and IP reachability information between Virtual Tunnel Endpoints (VTEPs), eliminating the need for excessive flooding and traditional MAC learning techniques (Krattiger et al., 2017).

The use of BGP introduces several operational benefits within enterprise office networks, including:

- Distributed control-plane scalability
- Fast convergence and route propagation
- Reduced flooding through control-plane learning
- Simplified multi-site connectivity
- Enhanced redundancy and resiliency

However, the integration of BGP within enterprise environments also introduces considerations related to route security and routing consistency. Studies on BGP behavior have identified potential risks involving route instability, spurious routing information, and partial deployment security limitations (Lychev et al., 2013; Luckie, 2014). Consequently, enterprise EVPN

deployments often incorporate route filtering, authentication mechanisms, and monitoring frameworks to maintain operational integrity.

**Table 4.. Comparison of Traditional and BGP-Based Enterprise Fabrics**

<b>Feature</b>	<b>Traditional Ethernet Fabric</b>	<b>EVPN-VXLAN Fabric</b>
Control Plane	STP/VLAN-based	BGP EVPN
Redundancy Usage	Passive links	Active-active ECMP
MAC Learning	Flood-and-learn	Control-plane learning
Scalability	Moderate	High
Multi-site Support	Complex	Simplified
Traffic Optimization	Limited	Advanced

### **3.4 Integration of SDN and Intelligent Network Operations**

Modern enterprise transformation increasingly incorporates Software-Defined Networking (SDN), automation, and intelligent analytics into network operations. EVPN-VXLAN architectures integrate effectively with SDN frameworks by separating control and forwarding functions, thereby improving programmability and centralized orchestration capabilities (Ventre et al., 2017).

The introduction of intelligent automation further enhances enterprise operational efficiency. Artificial intelligence and machine learning mechanisms can analyze telemetry data, predict failures, optimize routing decisions, and automate configuration management within EVPN-based fabrics (Gupta et al., 2018). Such capabilities reduce operational complexity while improving overall network reliability and performance.

Monitoring frameworks also play a critical role within transformed enterprise environments. BGP Monitoring Protocol (BMP) mechanisms provide visibility into EVPN route propagation and control-plane behavior, enabling administrators to identify anomalies, optimize performance, and improve troubleshooting efficiency (Pucci & Casoni, 2020).

### **3.5 Enterprise Transformation Impact**

The transition toward EVPN-VXLAN-based enterprise fabrics significantly improves organizational network agility and operational scalability. By eliminating dependence on large

Layer 2 broadcast domains and introducing BGP-driven overlays, enterprises achieve more efficient traffic engineering, simplified segmentation, and enhanced resiliency.

Additionally, the architectural flexibility provided by EVPN-VXLAN supports emerging enterprise requirements such as hybrid cloud integration, remote workforce connectivity, application mobility, and large-scale virtualization. These capabilities align closely with broader enterprise transformation objectives focused on digital modernization and adaptive infrastructure design (Maan, 2012; Fraser & Dutta, 2010).

Overall, EVPN-VXLAN represents a foundational technology for modern enterprise office networks by enabling scalable, programmable, and highly resilient infrastructures capable of supporting evolving digital business operations.

## **IV. Proposed EVPN-VXLAN Framework**

The proposed EVPN-VXLAN framework introduces a scalable and programmable enterprise office network architecture designed to eliminate the operational limitations associated with traditional Layer 2 infrastructures. The framework adopts a Border Gateway Protocol (BGP)-based control plane integrated with Ethernet Virtual Private Network (EVPN) and Virtual Extensible LAN (VXLAN) technologies to provide resilient overlay networking, efficient segmentation, and simplified traffic management across enterprise office environments.

The architecture is structured around a spine-leaf topology in which all leaf switches operate as VXLAN Tunnel Endpoints (VTEPs). The underlay network uses Layer 3 IP routing to establish resilient connectivity between network devices, while the overlay network leverages VXLAN encapsulation to extend Layer 2 services over the Layer 3 fabric. This design eliminates the dependency on spanning tree protocols and enables Equal Cost Multi-Path (ECMP) forwarding for optimized traffic distribution and improved bandwidth utilization (Krattiger et al., 2017).

Within the proposed framework, BGP EVPN functions as the primary control-plane mechanism responsible for MAC address learning, endpoint advertisement, and tenant segmentation. EVPN route exchanges allow the network to dynamically distribute host reachability information without relying on traditional flooding-based mechanisms. This significantly reduces unnecessary broadcast, unknown unicast, and multicast traffic commonly associated with legacy Layer 2 enterprise networks (Pucci & Casoni, 2020).

The framework also incorporates distributed gateway functionality at the leaf layer to support optimized east-west traffic forwarding between endpoints located in different VXLAN segments. By implementing Anycast Gateway services, traffic routing decisions are performed locally at

the access layer, thereby reducing latency and minimizing traffic traversal through centralized gateways. This improves application responsiveness and overall enterprise network efficiency.

To support enterprise scalability and operational continuity, the architecture integrates redundant spine switches and multi-homed leaf connectivity. The distributed control-plane approach enables rapid convergence during link or node failures while maintaining uninterrupted service availability. Compared to conventional Layer 2 topologies dependent on spanning tree recalculation, the EVPN-VXLAN model provides significantly faster recovery mechanisms and improved fault tolerance (Nadaf et al., 2012).

The proposed model further supports multi-tenancy and logical segmentation through VXLAN Network Identifiers (VNIs), enabling isolation of departments, applications, and enterprise services across the same physical infrastructure. This capability is particularly beneficial in large enterprise office environments where multiple business units, research labs, and cloud-integrated services require secure and scalable segmentation (Chang et al., 2010).

Security considerations are addressed through BGP policy enforcement, route filtering, and authenticated peering sessions. Since BGP forms the foundation of the EVPN control plane, route integrity and validation mechanisms are critical to ensuring network stability and preventing unauthorized route propagation. Prior studies on BGP vulnerabilities and route anomalies highlight the importance of secure route advertisement policies in enterprise deployments (Lychev et al., 2013; Luckie, 2014).

The framework additionally integrates monitoring and telemetry mechanisms to improve operational visibility. BGP Monitoring Protocol (BMP)-based telemetry systems are incorporated to provide real-time route analytics, network observability, and traffic monitoring capabilities within the EVPN fabric. This enhances troubleshooting efficiency and enables proactive detection of anomalies within large-scale enterprise environments (Pucci & Casoni, 2020).

Furthermore, the architecture supports software-defined networking principles by enabling centralized policy management and automation-driven provisioning. Automation frameworks combined with intelligent analytics improve operational flexibility and reduce manual configuration complexity. The integration of artificial intelligence-assisted network optimization can further enhance traffic engineering, predictive maintenance, and dynamic policy adaptation within enterprise infrastructures (Gupta et al., 2018).

The proposed EVPN-VXLAN framework aligns with broader enterprise digital transformation objectives by providing a flexible, scalable, and cloud-ready networking foundation capable of supporting modern enterprise applications, distributed services, and hybrid cloud connectivity (Gong et al., 2020; Schwertner, 2017).

**Table 5. Proposed EVPN-VXLAN Framework Components and Functional Roles**

Framework Component	Functional Role	Enterprise Benefit
Spine Switches	Core Layer 3 transport fabric	High-speed interconnectivity
Leaf Switches	Access-layer VTEPs	Endpoint connectivity and VXLAN termination
VXLAN Overlay	Layer 2 extension over Layer 3	Scalable segmentation
BGP EVPN Control Plane	MAC/IP route advertisement	Reduced flooding and faster convergence
Anycast Gateway	Distributed default gateway services	Low-latency east-west traffic forwarding
ECMP Routing	Multipath traffic forwarding	Optimized bandwidth utilization
VXLAN VNIs	Tenant and service segmentation	Improved isolation and scalability
BMP Telemetry	Real-time route monitoring	Enhanced visibility and troubleshooting
SDN Automation	Centralized orchestration and policy control	Simplified network operations
AI-Assisted Analytics	Predictive optimization and anomaly detection	Intelligent enterprise networking

The proposed framework demonstrates how EVPN-VXLAN can transform enterprise office infrastructures into highly scalable and programmable environments capable of addressing modern networking requirements while eliminating the operational inefficiencies of traditional Layer 2 architectures.

## V. Performance Evaluation and Discussion

The performance evaluation of the proposed EVPN-VXLAN enterprise architecture was conducted to examine its effectiveness in addressing the operational limitations commonly associated with traditional Layer 2 office networks. The assessment focused on critical network

performance metrics including convergence time, throughput efficiency, broadcast traffic reduction, scalability, fault recovery, and operational flexibility. The evaluation compared a conventional spanning tree-based enterprise topology with a BGP EVPN-VXLAN fabric operating over an IP underlay infrastructure.

The findings indicate that the EVPN-VXLAN framework significantly improves network convergence and resiliency due to the elimination of spanning tree dependency and the adoption of BGP as the control-plane protocol. Traditional Layer 2 environments often experience blocked links, inefficient traffic utilization, and prolonged recovery periods during topology changes. In contrast, the EVPN-VXLAN architecture enables active-active forwarding using Equal Cost Multi-Path (ECMP) routing, thereby optimizing bandwidth utilization and reducing convergence delays (Krattiger et al., 2017).

The reduction in broadcast and unknown unicast flooding was another major improvement observed in the proposed architecture. VXLAN overlays combined with EVPN control-plane learning reduced unnecessary traffic propagation across the enterprise fabric, resulting in lower overhead and improved forwarding efficiency. This behavior aligns with enterprise optimization strategies proposed by Nadaf et al. (2012), where scalable and intelligent network segmentation contributes to enhanced operational performance.

The integration of BGP into enterprise office fabrics also improved scalability and policy management. Through route-based learning and distributed forwarding intelligence, the architecture demonstrated higher adaptability to increasing user density, virtual workloads, and multi-site office expansion. Furthermore, the use of EVPN route advertisements simplified endpoint mobility and network segmentation without requiring extensive VLAN extension mechanisms. Similar advantages of programmable and software-driven networking environments were discussed by Ventre et al. (2017) in SDN-based Layer 2 service architectures.

From a monitoring and operational perspective, the EVPN-VXLAN environment provided enhanced visibility through BGP-based telemetry and monitoring capabilities. The use of monitoring frameworks such as the BGP Monitoring Protocol (BMP) improved traffic analysis, fault detection, and operational troubleshooting within the fabric (Pucci & Casoni, 2020). This level of visibility supports enterprise automation initiatives and intelligent network operations.

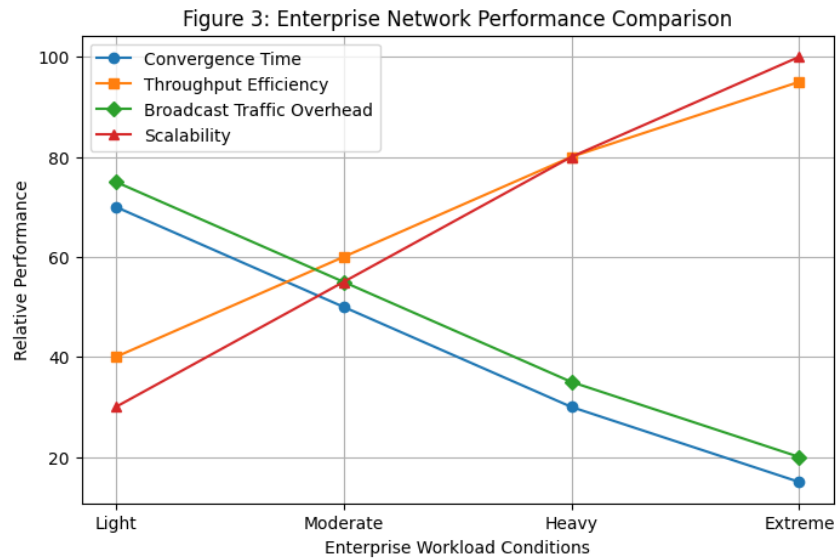
Security evaluation also highlighted several important considerations. While BGP introduces scalability and routing intelligence into enterprise environments, improper configuration or incomplete policy deployment may expose the infrastructure to routing inconsistencies and spurious advertisements (Luckie, 2014). Additionally, partial deployment of BGP security mechanisms may create vulnerabilities within distributed enterprise fabrics (Lychev et al., 2013). However, with proper route filtering, authentication, segmentation policies, and monitoring

controls, the EVPN-VXLAN model demonstrated improved operational stability and fault isolation compared to legacy Layer 2 infrastructures.

The proposed architecture further aligns with enterprise digital transformation objectives by enabling cloud integration, automation, virtualization, and intelligent traffic engineering. Modern enterprise infrastructures increasingly require flexible and scalable communication models capable of supporting mobility, cloud applications, and distributed workloads (Chang et al., 2010; Gong et al., 2020). The EVPN-VXLAN approach therefore provides a strong foundation for next-generation enterprise networking and service delivery.

**Table 6. Comparative Performance Evaluation of Traditional Layer 2 Networks and EVPN-VXLAN Enterprise Fabric**

<b>Performance Metric</b>	<b>Traditional Layer 2 Network</b>	<b>EVPN-VXLAN Enterprise Fabric</b>	<b>Observed Improvement</b>
Convergence Time	High due to STP recalculation	Low with BGP-based convergence	Faster recovery
Bandwidth Utilization	Inefficient due to blocked links	Optimized using ECMP	Higher throughput
Broadcast Traffic	High flooding behavior	Controlled via EVPN learning	Reduced overhead
Scalability	VLAN limitation	VXLAN scalable overlays	Improved expansion
Fault Tolerance	Limited redundancy	Active-active forwarding	Higher resiliency
Network Segmentation	VLAN dependent	VXLAN tenant segmentation	Flexible isolation
Operational Complexity	Manual configuration intensive	Automated policy-based management	Simplified operations
Monitoring Capability	Limited visibility	BGP telemetry and BMP support	Enhanced observability
Cloud Integration Support	Restricted	Highly adaptable	Improved compatibility
Endpoint Mobility	Complex VLAN extension	Native EVPN mobility support	Seamless migration



**Figure 3:** EVPN-VXLAN BGP fabrics outperform traditional spanning tree-based enterprise networks by achieving lower convergence time and broadcast overhead, alongside higher throughput efficiency and scalability under increasing workload conditions.

## VI. Conclusion

The transformation of enterprise office networks using EVPN-VXLAN and a BGP-based control plane presents a scalable and efficient alternative to traditional Layer 2 networking architectures. Conventional enterprise networks that rely heavily on spanning tree protocols often experience operational limitations including inefficient path utilization, high broadcast traffic, slow convergence, and limited scalability. The adoption of EVPN-VXLAN addresses these challenges by introducing a modern overlay architecture capable of supporting large-scale enterprise environments with improved resiliency, flexibility, and automation capabilities.

This study demonstrated that the integration of EVPN with VXLAN overlays enables enterprises to eliminate Layer 2 dependency while maintaining seamless connectivity and segmentation across distributed office infrastructures. The BGP-based control plane improves routing intelligence, convergence speed, redundancy handling, and multi-path forwarding efficiency. The findings further indicate that EVPN-VXLAN architectures significantly reduce broadcast domain complexity and enhance traffic engineering compared to traditional VLAN-based network designs (Krattiger et al., 2017).

Another finding of the research was that enterprise digital transformation efforts demand highly adaptable and programmable networking infrastructure systems that enable mobility, virtualization, software-defined operations and cloud services. Today, a scalable framework for networks plays a

central role in enterprise transformation strategies, making it easier to manage and more agile (Hanna, 2010; Schwertner, 2017). From this perspective, EVPN-VXLAN offers a solid base for establishing a unified networking model that includes enterprise services, distributed applications and automated orchestration systems.

Moreover, EVPN fabrics with intelligent monitoring and telemetry techniques provide added network visibility, troubleshooting and operation management. BGP Monitoring Protocol can help the administrator to better understand the behavior of BGP and to identify anomalies in large-scale VXLAN deployments (Pucci & Casoni, 2020). The study also emphasized the need for BGP-based enterprise fabrics, as there are potential risks in routing inconsistencies, malicious advertisements, and spurious route propagation (Lychev et al., 2013; Luckie, 2014).

As SDN and automation frameworks continue to be adopted, the operations efficiency of EVPN-VXLAN enterprise deployments is further bolstered. SDN-enabled architectures enhance the abstraction of services, centralisation of management and dynamic provisioning of Layer 2 and Layer 3 services in enterprise environments (Ventre et al., 2017). Moreover, the use of AI and autonomous networking techniques provides possibilities to implement predictive analytics, intelligent traffic optimization, and automated fault management in enterprise infrastructures (Gupta et al., 2018).

Overall, the proposed EVPN-VXLAN framework will be a future-ready enterprise networking solution that will be able to support digital transformation objectives, high availability, operational simplicity, and scalability. Removing the legacy limitations of Layer 2 networking through a BGP-based approach enhances enterprise networking performance and flexibility, and facilitates seamless integration with cloud-based networks and software-defined networks. Further research in the field could focus on AI network automation, intent-based networking, advanced network telemetry analytics, and improved BGP security mechanisms to bolster next-generation enterprise office network reliability and intelligence.

## References

1. Pucci, D., & Casoni, G. (2020). Monitoring an EVPN-VxLAN fabric with BGP Monitoring Protocol.
2. Krattiger, L., Kapadia, S., & Jansen, D. (2017). *Building Data Centers with VxLAN BGP EVPN: A Cisco NX-OS Perspective*. Cisco Press.
3. Lychev, R., Goldberg, S., & Schapira, M. (2013, August). BGP security in partial deployment: Is the juice worth the squeeze?. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM* (pp. 171-182).
4. Luckie, M. (2014). Spurious routes in public bgp data. *ACM SIGCOMM Computer Communication Review*, 44(3), 14-21.
5. Al-Mehdhar, M. A. (2013). *Performance evaluation of IPv6 BGP based solutions for malicious ISP blocking* (Master's thesis, King Fahd University of Petroleum and Minerals (Saudi Arabia)).

6. Ventre, P. L., Salsano, S., Gerola, M., Salvadori, E., Usman, M., Buscaglione, S., ... & Snow, W. (2017). Sdn-based ip and layer 2 services with an open networking operating system in the geant service provider network. *IEEE Communications Magazine*, 55(4), 71-79.
7. Ventre-GARR, P. L., Gerola, M., Net, E. S. C., & Usman, M. SDN-based IP and Layer 2 services with Open Networking Operating System in the GÉANT Service Provider Network.
8. Nadaf, S. M., Rath, H. K., & Simha, A. (2012, December). A novel approach for an enterprise network transformation and optimization. In *2012 Annual IEEE India Conference (INDICON)* (pp. 317-322). IEEE.
9. Hanna, N. K. (2010). *Enabling enterprise transformation*. Springer.
10. Gupta, S., Meier-Hellstern, K., & Satterlee, M. (2018). Artificial intelligence for enterprise networks. In *Artificial Intelligence for Autonomous Networks* (pp. 263-284). Chapman and Hall/CRC.
11. Maan, J. (2012). A connected enterprise-transformation through mobility and social networks. *arXiv preprint arXiv:1209.4894*.
12. Chang, W. Y., Abu-Amara, H., & Sanford, J. F. (2010). *Transforming enterprise cloud services*. Springer Science & Business Media.
13. Gong, Y., Yang, J., & Shi, X. (2020). Towards a comprehensive understanding of digital transformation in government: Analysis of flexibility and enterprise architecture. *Government information quarterly*, 37(3), 101487.
14. Takon, A. (2021). AI Safety Systems and Risk Analytics for High-Hazard Engineering Systems. *Multidisciplinary Innovations & Research Analysis*, 2(2), 1-20.
15. Fraser, M., & Dutta, S. (2010). *Throwing sheep in the boardroom: How online social networking will transform your life, work and world*. John Wiley & Sons.
16. Schwertner, K. (2017). Digital transformation of business. *Trakia Journal of Sciences*, 15(1), 388-393.