RESEARCH
Influence and insight
through social media

December 2024

NETWORK FABRICS

The Foundation for Scaling and Securing Today's Distributed Enterprises

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

SECTION I: THE RISE OF THE DISTRIBUTED ENTERPRISE

In the past decade, businesses have transformed into distributed enterprises characterized by a decentralized structure facilitated by technological advancements. This transformation underscores a new era when businesses are not confined to a single location or a standard global workflow but are spread across multiple geographies and digital platforms. Several factors have contributed to the rise of the distributed enterprise, which ZK Research explores in this paper.

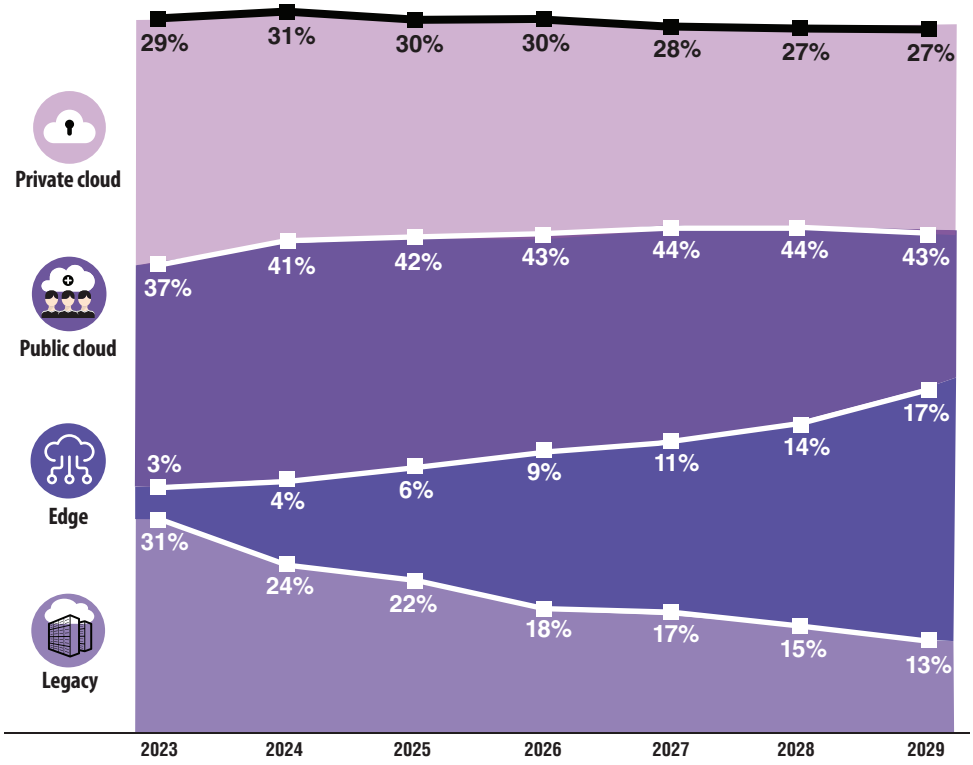
The following macro trends are driving the distributed enterprise:

Continuing the Trend Toward Decentralization

Many enterprises have accelerated their adoption of cloud-based solutions. The shift toward hybrid cloud infrastructure allows companies to balance on-premises resources with cloud capabilities, offering flexibility, scalability, and enhanced collaboration among teams across different locations.

Edge computing further supports the distributed enterprise by bringing compute and data storage closer to the location where it is needed, reducing latency and improving speed. This is crucial for industries that require real-time processing of data, such as healthcare, finance, and manufacturing. Exhibit 1 highlights how compute will continue to decentralize and grow at the edge, enabling companies to decentralize further.

Exhibit 1: Edge Computing Is on the Rise



ZK Research 2024 Cloud Computing Forecast

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

The Changing Nature of Work

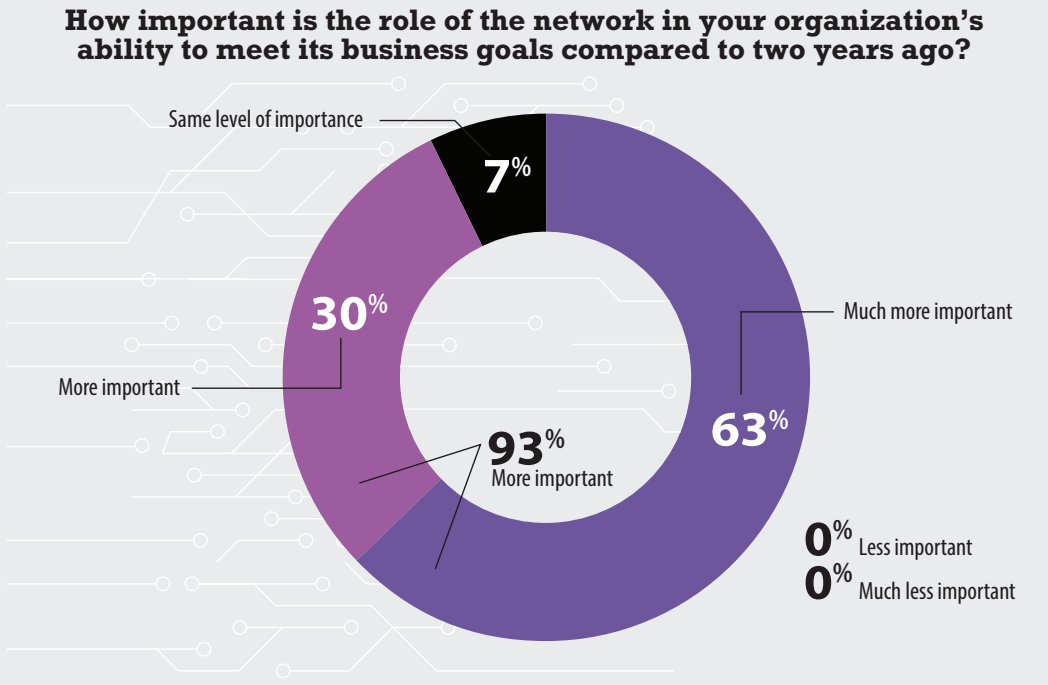
When the pandemic ended, the business world had shifted exclusively to a model where users worked from home. Two years ago, 91% of respondents to a ZK Research study stated they would have employees work from home two to three days a week. Since then, the business world has done an about-face, with many organizations mandating that people return to the office. Which will be the long-term work model? The answer is unknown, but companies need IT agility to adapt to the continually changing nature of work.

The Proliferation of Internet of Things (IoT) Endpoints

Virtually everything is being connected today. Automobiles, lighting systems, appliances, healthcare equipment, and more are connected to company networks. The ZK Research 2024 IoT Forecast predicts that 30 billion connected devices will be connected by 2030, up from 16 billion today. IoT creates new experiences and generates significant volumes of data.

This shift toward distributed architectures has made businesses increasingly network-centric. In a joint ZK Research/Cube Research study, 93% of organizations acknowledged that the network has become more critical to business operations compared to two years ago (Exhibit 2). This escalation highlights the network's role as the backbone of modern enterprise strategies, enabling seamless connectivity and integration across various platforms and devices.

Exhibit 2: Network Value Rises



ZK Research/Cube Research 2024 AI Networking Study

Companies must rethink traditional networking and advocate for architectures that align with the demands of a more connected, data-driven world.

However, the complexity of these networks continues to escalate. As enterprises evolve, their networks must accommodate a growing number of connected devices, applications, and data flows, complicating network management, security, and performance optimization. Traditional networking solutions, while still functional, are becoming increasingly inadequate at addressing these contemporary challenges.

The network architecture that supports modern distributed enterprises is primarily based on centralized control and hierarchical models and has largely remained unchanged for decades. However, in today's dynamic business environment, these models can impede innovation and rapid response to changing demands. Therefore, there is a growing consensus that merely adding layers to an old architecture is not sufficient.

The Need for a New Approach to Networking

Recognizing these challenges, there is an increasing call for a fundamental shift in how network architectures are conceived and deployed. The need for a new approach to networking—one that embraces the principles of distribution, decentralization, and democratization—is evident. This new approach should be flexible enough to manage the dynamic nature of data flows and robust enough to handle a vast array of devices and applications seamlessly.

As businesses continue to navigate this era of digital transformation, adopting a forward-thinking approach to network design will be crucial. Doing so involves embracing new technologies, shifting toward adaptive frameworks, and investing in innovative solutions that support the distributed nature of modern enterprises.

The rise of the distributed enterprise marks a significant inflection point in business evolution. To thrive in this new landscape, companies must rethink traditional networking and advocate for architectures that align with the demands of a more connected, data-driven world. One can't run a digital business on a legacy network. Embracing these changes will be essential for businesses aiming to remain competitive and responsive in a rapidly evolving market.

SECTION II: THE CHALLENGE WITH LEGACY NETWORKS

The current approach to network architecture has been in place for more than 40 years and was designed to support client-server computing. The compute industry has seen many major shifts—from branch computing, to virtualization, to cloud and distributed computing. In this time, networking as a paradigm has remained largely the same. Speeds have increased, as have densities. However, fundamental thinking about design and architecture has not. These are some of the limitations with current networks:

Historic Design Constraints

Legacy networks were conceived in an era dominated by on-premises resources. At that time, most workers, applications, and data were physically located within company facilities. Such networks

Operational inefficiency is a hallmark of a legacy network.

were optimized for internal communications and data exchange within a well-defined boundary. However, today's work environment is vastly different, with remote work becoming prevalent, cloud-based applications integral, mobility having become the norm, and data residing across various geographical locations. Consequently, the original design of these networks is mismatched with current demands, which require flexibility, scalability, and remote accessibility.

Operationally Intensive Manual Configuration

Operational inefficiency is a hallmark of a legacy network. These networks often require cumbersome manual configurations, which are time-consuming and prone to human error. In fact, ZK Research studies have found that human error is still the top cause of unplanned downtime. The lack of automation in traditional networks means that network professionals must spend significant amounts of time on routine maintenance and updates, diverting resources away from strategic initiatives. Additionally, over the years, innovation within these networks has primarily been executed by adding new protocols. This practice of "bolting on" enhancements has led to a complex web of protocols that complicates the network infrastructure, escalating operational difficulties and increasing the risk of configuration errors.

Security as an Overlay to the Network

One of the most significant drawbacks of legacy networks is the security model, where security is typically bolted on to the existing network infrastructure. This design results in several vulnerabilities. For instance, in the event of a security breach, threats can rapidly spread laterally across the network, compromising multiple systems and data repositories. Moreover, given the increasing sophistication of cyber threats, relying on patchwork security solutions is insufficient for effective protection.

Lack of Agility and Integration

Legacy networks often lack the agility required to support dynamic business environments, which is almost every organization today. Businesses require networks that can quickly adapt to changing workloads, integrate seamlessly with cloud services, and support an increasing number of connected devices. Legacy architectures struggle in these areas, leading to delays in deployment and scaling and ultimately hindering business operations.

Furthermore, these networks are typically deployed in silos, such as campus, Wi-Fi, data center, and WAN. This fragmented approach makes consistent policy management challenging and complicates the implementation of overarching security strategies. Each siloed segment may operate under different rules and configurations, necessitating more intricate coordination and increasing the likelihood of security lapses.

Modern enterprises require network solutions that provide superior agility, robust security, operational efficiency, and effective resource utilization.

Inefficient Resource Utilization

The traditional active-passive configuration of legacy networks fosters inefficiencies by causing enterprises to over-provision resources. This design, which was intended to provide redundancy and ensure uptime, often results in the underutilization of network ports and infrastructure. Consequently, businesses incur unnecessary costs by investing in and maintaining unused or underutilized resources to safeguard against potential service disruptions. This is due to the use of the Spanning Tree Protocol (STP), which prevents routing loops and broadcast radiation by disabling ports that are not part of the spanning tree. These disabled ports are only made active in the event of a failure of one of the active ports. This inefficient use of network ports requires companies to purchase many more ports than necessary.

The limitations of legacy network architectures have existed for years but are becoming increasingly detrimental to organizations striving to remain competitive in the digital age. Modern enterprises require network solutions that provide superior agility, robust security, operational efficiency, and effective resource utilization. Transitioning to a more flexible approach to network architecture can address these challenges. Such networks are designed to be inherently agile, facilitating automated processes, centralized management, and enhanced security postures that can adapt to the fast-evolving digital landscape. Embracing a network fabric is critical for enterprises aiming to thrive in today's fast-moving digital landscape.

SECTION III: NETWORK FABRICS REVOLUTIONIZE NETWORK CONNECTIVITY

A network fabric is a virtualized overlay that can enable connectivity to any part of the distributed enterprise simply, quickly, and with a consistent user experience. Juxtapose this with legacy networks that often dictate that the user is the integration point for managing the complexity. In contrast, a fabric uses the network to make intelligent decisions and masks the complexity from the user.

Not all network fabrics are the same. Two common variants include Shortest Path Bridging (SPB) fabrics and IP fabrics, such as EVPN/VXLAN fabrics. SPB fabrics are primarily Layer 2 fabrics, though some can span multiple areas and leverage IS-IS as the control plane. SPB fabrics, due to their simplicity, flexibility, and zero-touch automation, are very well suited to enterprise networks and their broad use cases. IP fabrics, which were designed for communications service providers, are better suited to and often restricted for use in Layer 3 data centers. This paper focuses on SPB fabrics.

Network fabric technology based on SPB 802.1Q, an IEEE networking standard, reduces the protocol stack required for most networks to a single protocol that significantly simplifies network design and operation. SPB enables efficient routing by sending data along the shortest paths within the network. This approach eliminates the need for complex manual configurations that are commonplace in traditional networks. Consequently, SPB reduces operational overhead and minimizes errors, making network management more straightforward and efficient.

Benefits of an SPB network fabric include the following:

Virtual Connectivity Across the Network

One of the top features of a network fabric is its ability to virtually connect every point within the network to every other point. This simplified, end-to-end connectivity ensures that data can flow seamlessly among devices, applications, and users. Such connectivity is crucial for supporting the diverse needs of modern enterprises, which often span multiple geographic locations and encompass a range of devices, from campus systems and remote branches to IoT endpoints.

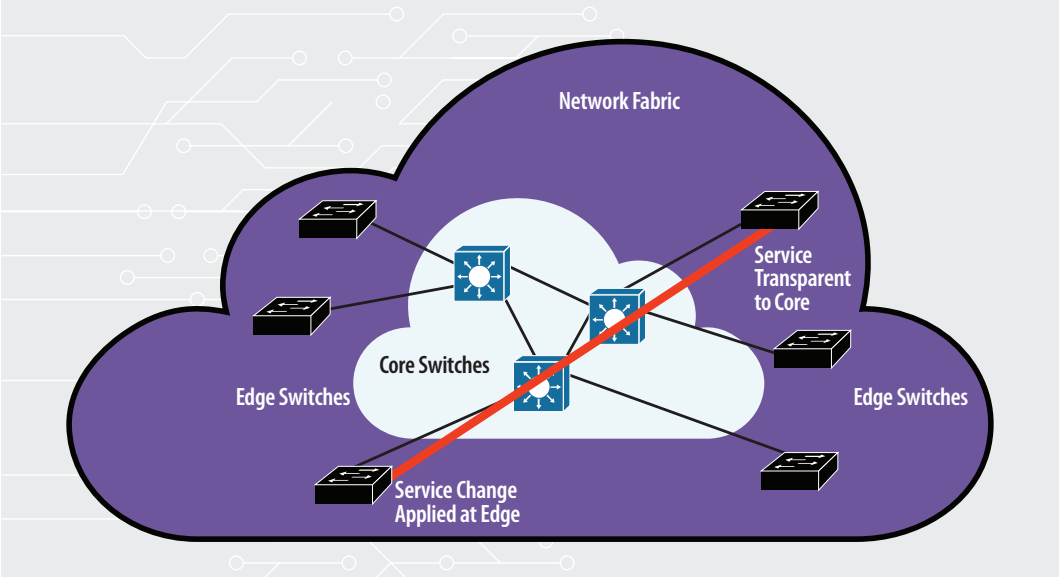
Edge Provisioning and a Transparent Core

In traditional networks, each node in the network needs to be configured, inspect the traffic, and move it to the next node—adding unnecessary latency and overhead. SPB network fabric approaches utilize an architecture where provisioning is implemented at the edge of the network, leaving the core as a zero-touch, high-speed conduit for data (Exhibit 3). This design leverages intelligence at the edge, enabling more efficient data processing and reduced latency. The hands-free core simplifies network operation by focusing on high-speed data transit without the complexities of traditional networks, where core configurations can be intricate and resource intensive.

Extensibility Across the Distributed Enterprise

The extensibility of network fabrics is a critical advantage, particularly for enterprises distributed across various environments. Network fabrics can extend seamlessly across campuses, connect IoT

Exhibit 3: Network Fabrics Simplify Operations



ZK Research, 2024

endpoints, and traverse wide-area networks (WANs) to reach remote branches. This extensive range helps ensure consistent connectivity and performance across the organization, supporting a unified strategy for network and resource access and security.

The rise of the network fabric represents a modern approach to networking architecture that addresses the challenges posed by legacy systems.

Security and Zero-Trust Integration

Security is an integral aspect of network fabric design. By incorporating security measures directly into the network architecture, deploying a zero-trust security model becomes simpler and more effective. In a zero-trust framework, every user and device must be authenticated and authorized before gaining network or application access, minimizing the risk of unauthorized access. This built-in security enhances the network's overall integrity and protects sensitive data.

Automation and Reduced Human Error

Network fabrics are designed for easy automation, streamlining network management tasks, and greatly reducing the potential for human error and the time spent resolving conflicts and errors. Automation facilitates rapid deployment, scaling, and configuration adjustments, freeing network administrators from manual processes. As a result, organizations can achieve higher levels of efficiency and accuracy in network operations, ensuring consistent performance and reliability.

Active-Active Configuration and Resource Efficiency

Another significant benefit of network fabric approaches is the adoption of active-active configurations. Unlike traditional active-passive setups that require redundant resources for failover, active-active configurations utilize all resources concurrently. This design minimizes wasted capacity and reduces the number of necessary ports, optimizing the network's cost-effectiveness and resource allocation.

Improved User Experience

Finally, the approach of network fabrics positively impacts network performance and end-user experience. By providing low-latency, high-throughput paths for data, applications can operate more efficiently, improving user experiences and productivity. The ability to automatically adjust to accommodate varying workloads ensures that application performance remains consistent, even as network demands fluctuate.

The rise of the network fabric represents a modern approach to networking architecture that addresses the challenges posed by legacy systems. This evolves the network to meet the demands of highly agile digital organizations. By leveraging SPB and integrated security, network fabrics offer a simplified, scalable, and secure foundation for modern enterprises. With their ease of automation, built-in security, and resource efficiency, network fabrics are poised to support the demands of an ever-changing digital landscape.

SECTION IV: EXTREME NETWORKS IS A PIONEER IN NETWORK FABRICS

Extreme Networks has disrupted the space with the only end-to-end solution that spans campus, data center, and branch.

Extreme Networks pioneered network fabric technology and is currently the market leader in SPB-based deployments. While most incumbent vendors have chosen to utilize legacy systems, Extreme has disrupted the space with the only end-to-end solution that spans campus, data center, and branch.

Extreme Fabric was designed based on the following three principles:

Unify

Networks are heterogenous and need to be extensible. Therefore, the fabric overlay must span the entire network end to end from campus and data center to branch locations with SD-WAN. Extreme Fabric works with wired, wireless, WAN devices, IoT, and third-party switches. With more than 5,000 deployments worldwide, it delivers a full suite of network services including Layer 2, Layer 3, and IP Multicast.

Extreme's Fabric is included free with all of its Universal Switches. Fabric provides the greatest benefits when it is used holistically across campus, data center, and branch. However, a fabric can add simplicity, automation, and security in any use case where a VLAN might be useful. Extreme Fabric allows customers to deploy at their own pace, which may begin with a more traditional architecture that evolves to fabric over time. For example, an organization might

- deploy fabric only at its campus core where security and resilience are often most critical,
- connect a campus and data center to improve network access security as employees return to the office,
- or connect specific edge segments, such as a guest or IoT segment, across campus, data center, and branch, where either traffic isolation, time to service, or uptime are critical.

Automate

As networks become more complex and distributed, the fabric must use automation to eliminate the manual, error-prone configurations found in box-by-box approaches. Zero-touch provisioning and auto-configuration make Extreme Fabric easy to deploy and scale. This automates the creation of new network segments, shortest paths, instant self-healing, and device onboarding.

The network also must stay up at all times. Because Extreme Fabric is based on SPB and uses only one protocol, should a cable, port, or switch fail, the network reconverges over new switching paths and traffic is redirected typically within 200 milliseconds. This sub-second convergence helps prevent unplanned and planned downtime, such as during upgrades or maintenance, so that the network operation is not disrupted.

ExtremeCloud IQ, Extreme's visual management environment for its fabric, is natively designed to provide end-to-end network visibility, fabric monitoring, and management capabilities. It provides in-depth details about the performance of applications and the network.

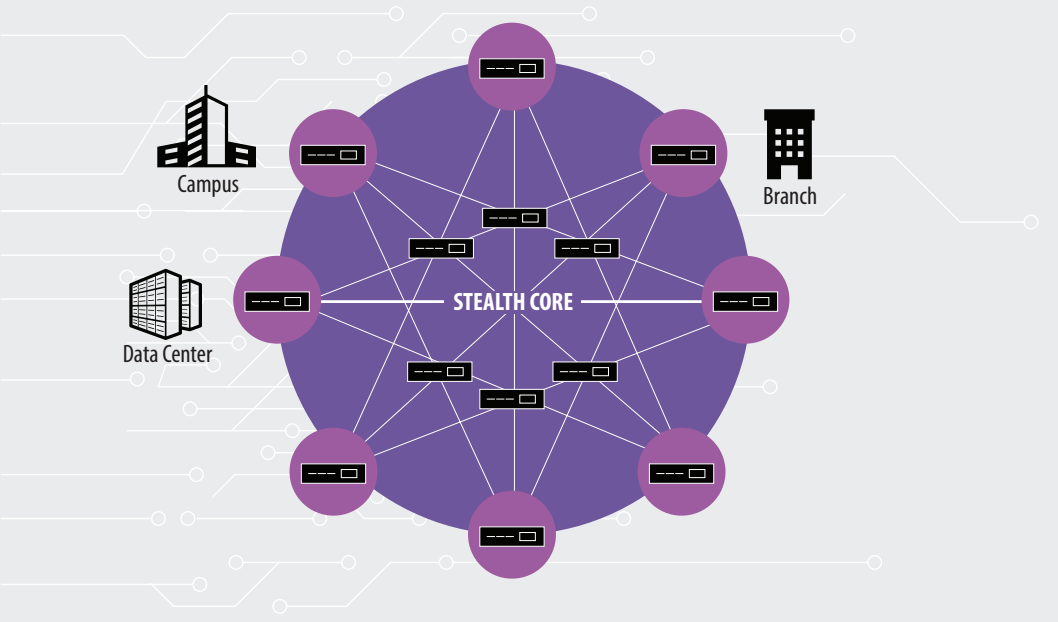
Secure

Large complex networks broaden the potential attack surface. Consequently, a network fabric must be capable of preventing and reducing the impact of cyberattacks. Extreme Fabric provides an intrinsically secure network with two key capabilities: automated micro-segmentation and stealth topology.

Micro-segmentation enables organizations to partition applications, data, and users easily and at scale. This differs from traditional segmentation approaches, which are typically manual and rely on broad zones for control. Micro-segmentation facilitates the creation of secure, isolated, end-to-end virtual segments to prevent bad actors from moving laterally within the network. Users, devices, and services are bundled into these segments, which are isolated from each other. Additionally, Extreme Fabric extends micro-segmented network services to the edge only as required and only for the duration of use. As usage terminates or endpoint devices disconnect, services are spun down. This provides a fully automated way to reduce the network's attack surface.

Stealth topology also reduces the attack surface by hiding the network core from IP scans and attackers. Extreme Fabric's core is built once and then remains "hands-off." Configuration and provisioning are done only at the edge. These updates are then dynamically propagated throughout the network over a stealth core (Exhibit 4). The topology is invisible from an IP perspective, as there are no inherent IP routes or hop-by-hop paths to trace.

Exhibit 4: Extreme Fabric Operates from the Edge



Extreme Networks and ZK Research, 2024

SECTION V: FABRIC USE CASES

Extreme Fabric is widely deployed and used by more than 5,000 customers today. This section presents several customer deployments that highlight the value customers across the globe have realized with the network fabric.

Extreme Fabric is widely deployed and used by more than 5,000 customers today.

Case Study: Enhancing Digital Equity at San Diego Community College District

The San Diego Community College District (SDCCD), one of California's most prominent educational institutions, serves over 100,000 students annually across 14 physical locations in San Diego County. With the imperative to deliver consistent digital experiences for both students and faculty, the district's IT department faced a multitude of challenges. These included ensuring a uniform digital experience for more than 80,000 users and providing robust connectivity to manage thousands of devices, video streaming, and diverse applications. Additionally, there was a need for improved troubleshooting and monitoring of network performance, alongside a scalable solution that would adapt to the district's growth and expansion.

As highlighted by Jon Ambrosia, the enterprise network specialist at SDCCD, the integration of modern technologies such as SPB positioned Extreme Networks as an unmatched partner, allowing for comprehensive visibility and swift responsiveness to network demands.

To tackle these challenges, SDCCD implemented a suite of Extreme solutions, including Extreme Fabric, ExtremeCloud IQ, and Extreme Wired and Wireless. The results were transformative; the district achieved digital equity for all students and faculty, facilitating a reliable and resilient infrastructure that supported critical applications and enhanced digital experiences.

Furthermore, the scalable fabric solution underscores SDCCD's commitment to growth and innovation, ensuring ongoing support for future initiatives. The enhanced visibility into network performance allowed for quicker maintenance and troubleshooting, ultimately fostering a more connected and efficient educational environment. Through these advancements, SDCCD has positioned itself to effectively meet its community's evolving needs.

Case Study: Revolutionizing Connectivity and Digital Applications at Dubai World Trade Centre

The Dubai World Trade Centre (DWTC) has been a cornerstone of Dubai's business tourism and trade since its inception in 1979. Spanning an impressive 1.3 million square feet, the campus comprises exhibition halls and smart office buildings, hosting more than 500 events annually. As the demand for mega-events intensified, DWTC faced multiple challenges, including the need to reduce convergence times, streamline network configurations, and improve overall network resiliency.

Farid Farouq, DWTC's vice president of IT, procurement, and contracts, emphasized the importance of setting new standards for event hosting. To address these challenges, DWTC turned to Extreme's networking solutions, aiming to provide a world-class experience for exhibitors and

The advanced features of Extreme Fabric facilitate simplified network operations, enabling the swift deployment of new services and effective network virtualization.

visitors while simplifying network management. With the implementation of Extreme Fabric and ExtremeCloud IQ, DWTC achieved secure, reliable, and scalable connectivity.

The new network infrastructure supports high-bandwidth digital applications such as contactless engagement technologies and high-definition video, which are essential for modern event experiences. Additionally, DWTC reliably operates multiple CCTV cameras, enhancing security and compliance. The advanced features of Extreme Fabric facilitate simplified network operations, enabling the swift deployment of new services and effective network virtualization. Furthermore, the real-time insights provided by ExtremeCloud IQ empower DWTC to optimize its network capabilities and manage venue capacity efficiently, ensuring a seamless experience for all users and solidifying its position as a premier event destination.

Case Study: Ensuring Reliable Healthcare Connectivity at ADRZ

ADRZ, a regional hospital formed in The Netherlands following a merger, provides vital general and emergency care across its locations in Goes, Vlissingen, and Zierikzee. With more than 2,250 employees, 180 medical specialists, and 140 volunteers, ADRZ is dedicated to delivering high-quality, accessible healthcare, especially within regions characterized by significant distances between population centers. In supporting this mission, the hospital faced critical challenges related to maintaining a 24/7 operational network; accommodating an increasing number of users, devices, and applications; and implementing robust security measures for proactive troubleshooting.

To resolve these challenges, ADRZ deployed a comprehensive suite of Extreme solutions, including Extreme Wireless, Extreme Wired, and Extreme Fabric. This transformation resulted in a reliable network that has consistently operated without failure for more than a decade, which is essential to meet the demands of a busy hospital environment. The scalable network infrastructure allows for growth without requiring additional IT personnel or complicated solutions, while automated segmentation and proactive management features significantly reduce the risk of human error.

Mark van Strien, senior network administrator at ADRZ, highlighted the network's impressive reliability, stating, "The core network of our hospital hasn't been down for about 11 years now." This solid foundation enhances the quality of care and ensures that ADRZ remains prepared to meet the ongoing needs of its patients and healthcare professionals.

SECTION VI: CONCLUSION AND RECOMMENDATIONS

Enterprises are becoming increasingly digitized, putting pressure on network operations. All of the digital building blocks—cloud, mobility, IoT, and AI—are network-centric, resulting in the network becoming the underlying foundation for digital transformation. However, the traditional approach to networking architecture has been around for decades and was built when best-effort services were the norm.

Distributed enterprises must rethink the network and deploy one that is highly agile and intrinsically secure and can meet the company's demands. A network fabric is the right approach today, and businesses that choose to deploy it will realize the following benefits:

Simplified operations: Network fabrics offer robust and scalable networks that eliminate complexity and improve IT productivity.

Faster time to service: A network fabric improves service agility and minimizes unplanned downtime.

Highly secure: A network fabric is built to be secure, protect against attacks, and deliver superior service availability without impacting the user experience.

To help decision makers chart their path to a network fabric, ZK Research makes the following recommendations:

Embrace the concept of a network fabric. Moving away from a "tried and true" system can be difficult. As mentioned earlier, the current network design most companies use has been in place for decades, but it's well past its prime. Networks are manually intensive and prone to human error, and this can hold companies back from moving forward with digital initiatives. Embracing a network fabric is the right decision for companies today, as it modernizes the network—which, for most companies, is long overdue.

Automate network operations. All businesses want to move with speed, and the majority of IT has embraced automation. Developers can automate the creation of code; IT pros can spin up containerized compute nodes instantly; and the cloud enables services to be deployed anywhere, instantly. Network operations must embrace automation to keep up with the rest of IT. Network fabrics are built with automation in mind, so changes can be made once instead of the typical box-by-box methodology that can often take months to complete network wide.

Rethink your network vendors. When refreshing a network, the easiest choice is often to stick with the incumbent vendor. However, the market leader is rarely the one that disrupts markets, as doing so can harm its overall business. Therefore, evaluate your next vendor based on its ability to automate and secure the network—but in a way that's operationally simple.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314