



Digital Transformation on the Edge: Are the Hidden Limitations of Conventional Network Design and Traditional PoE Switches Threatening Your ROI?

How Modern LAN Principles Help Organizations Avoid Digital Transformation Pitfalls to Improve Return on Investment

A NVT Phybridge Whitepaper

[McKinsey & Company](#), a global management consulting firm providing advisory services to businesses, governments, and institutions, has published multiple reports indicating that many digital transformation initiatives fail to achieve their expected ROI. For example, a McKinsey & Company survey found that less than 30% of digital transformation projects meet their objectives.¹

This whitepaper will explore the challenges organizations face in achieving an acceptable return on investment from their digital transformation initiatives, recommendations for improving success rates, and how Modern LAN Principles can support this success. The information included in this whitepaper is from reports by McKinsey & Company, [Boston Consulting Group \(BCG\)](#), [Gartner](#), [Deloitte](#), [PwC](#), [Harvard Business Review](#), and [Frost & Sullivan](#).

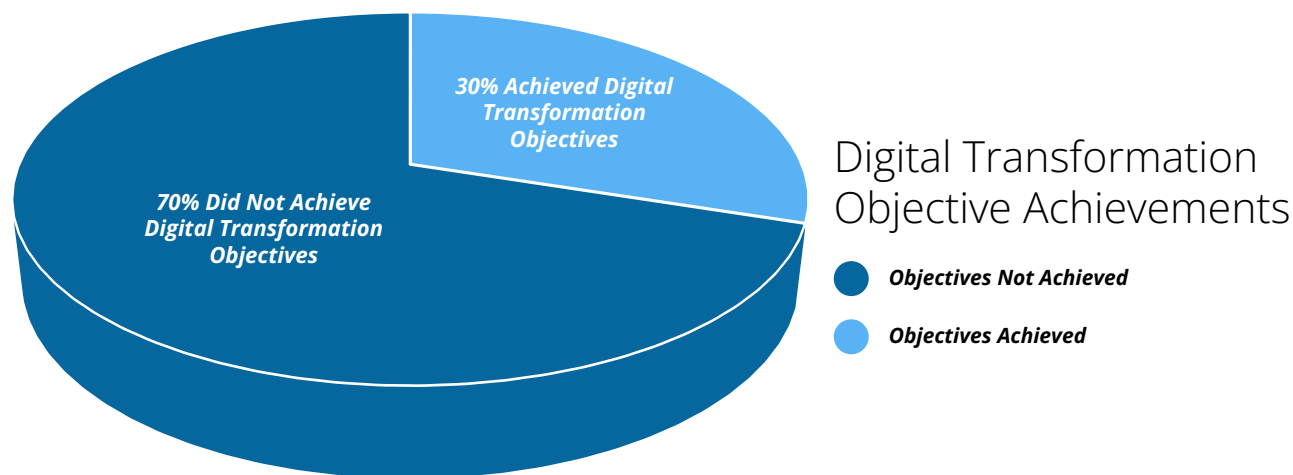


Contents

Digital Transformation Insights, Trends & ROI Challenges	1
The Evolving Role of Financial Decision Makers	1
Common Digital Transformation Challenges	1
Increased Complexity and Stress on IT Teams	2
Evolution of LAN Design	3
Why Are We Still Using Thirty-Five-Year-Old LAN Design Thinking?	3
Network Vulnerability & Security Risks	4
Modern LAN Design for Better Digital Transformation Outcomes	5
Implementing A Purpose-Built and Modern LAN Design	7
Benefits of Modern LAN Principles	8
Tested and Proven Strategies	10
Avoid Potential Conflict of Interest	10
About Us - Our Mission	10
Bibliography	11

Digital Transformation Insights, Trends & ROI Challenges

According to a McKinsey & Company survey, less than 30% of digital transformation projects meet their objectives, highlighting the difficulty in achieving expected ROI, with common issues including the need for more precise goals, insufficient leadership, and resistance to change.² A report from BCG found that only one in three digital transformation projects result in improved performance and sustained change, with major challenges often stemming from cultural resistance, lack of digital skills, and inadequate change management.³



The Evolving Role of Financial Decision Makers

Gartner highlights that CFOs and other financial leaders are increasingly involved in evaluating and overseeing digital transformation investments. Organizations are including these stakeholders to ensure projects are financially viable and aligned with business objectives. Financial leaders are becoming critical stakeholders in setting digital strategies and ensuring measurable investment returns.⁴ However, while involving financial decision-makers is a step in the right direction, we must also explore the other factors contributing to lower returns on investment. To better understand the situation, we should examine the root causes of these challenges and identify ways to address them.

Common Digital Transformation Challenges

A report from PWC highlights that many organizations struggle to achieve desired digital transformation outcomes despite significant investments. It identifies misalignment with business strategy, inadequate measurement of success, and cultural resistance as core issues.⁵ In addition, experts at Harvard Business Review found that many high-profile digital transformations fail due to poor financial oversight and misalignment with business objectives.⁶ Research firms agree that financial leaders must be involved in planning and decision-making to ensure projects are financially sound and strategically aligned.

Organizations often need to more heavily consider the cost, complexity, and risk associated with local area network (LAN) requirements. Establishing a secure, robust, and high-performance network to support new endpoints and applications is the first step, and these unforeseen costs can often erode budget availability for ROI drivers (endpoints, applications, and application adoption). Many organizations fail to fully anticipate the

complexities, expenses, and security vulnerabilities of upgrading networks to support new IP endpoints, leading to significant financial and operational challenges. Additionally, the integration challenges of infrastructure upgrades often lead to higher-than-expected costs. While initial cost estimates may seem reasonable, additional costs often arise from necessary network improvements, such as enhanced PoE (Power over Ethernet) switches, additional cabling, and improved network security measures. Unplanned costs can also stem from the need for network redesign, additional hardware, and extensive testing and validation processes.

Frost & Sullivan reports on IP endpoint deployments, underlining the importance of considering all potential costs, including network downtime, training, and ongoing maintenance costs. Frost & Sullivan provide case studies where cost overruns were primarily due to inadequate initial assessments and planning.⁷

Increased Complexity and Stress on IT Teams

IT teams can struggle with the increased complexity of network management as more IP endpoints are deployed while integrating new technologies with legacy systems adds complexity and stress. The proliferation of IP endpoints increases the attack surface, making network management and security more challenging. IT teams are under greater pressure to ensure robust security measures are in place while managing an ever-growing number of devices. Many studies and reports highlight the increased complexity and stress experienced by IT teams as organizations undergo digital transformation and deploy more IP endpoints on their networks. Here are some key reports and their findings:

- Gartner shares its findings on the increasing complexity IT teams face during digital transformation, stating that deploying additional IP endpoints, such as IP phones, cameras, and IoT devices, significantly increases the workload on IT teams, leading to higher stress levels and the need for enhanced skills. Gartner emphasizes the importance of automation, improved IT processes, innovation, and continuous training to help IT teams manage this increased complexity.⁸
- The Ponemon Institute found that digital transformation efforts significantly increase workload and stress for IT professionals. The study notes that IT teams are often not adequately prepared for the scale of these transformations.⁹
- A Forrester report on digital transformation highlights the strain on IT teams due to the increased complexity of managing modern, IP-based networks. Forrester reports that IT departments face challenges such as maintaining network performance, ensuring security, and managing diverse endpoints.¹⁰
- Frost & Sullivan reports that traditional network design methods have not advanced as quickly as the IP endpoints being deployed, resulting in higher costs, greater complexity, and more stress on IT teams. They highlight the need to consider advancements in network design and PoE capabilities.¹¹

Many of today's digital transformation challenges and the lack of adequate ROI can be attributed to LAN design practices and traditional PoE capabilities not evolving as quickly as the endpoints deployed. It is important to understand the history of LAN design, the reasons traditional methods have not kept pace with today's network requirements, and what organizations can do to improve digital transformation outcomes while reducing the stress on IT teams.

Evolution of LAN Design

In 1989, Kalpana introduced the first multi-port LAN switch. Early LANs were designed to connect data terminals (such as PCs) to a central mainframe or server, facilitating essential data sharing and communication. These networks typically used Ethernet over coaxial cables or early twisted-pair cabling, with limited bandwidth and basic switch/router configurations. The network's primary function was to support basic file sharing, email, and print services with low complexity and security requirements.

As computing needs grew, networks began to support more diverse devices, including printers, scanners, WiFi access points, and early VoIP phones. Networks evolved to use faster Ethernet standards (such as 100 Mbps Fast Ethernet and 1 Gbps Gigabit Ethernet) and more sophisticated network infrastructure, including advanced switches and routers.

Today, modern networks support a wide range of IP endpoints, including IP phones, IP cameras, IoT devices, smart appliances, and more. The increase in video conferencing, cloud computing, IoT, and AI applications demands higher bandwidth and more reliable network performance. With more endpoints, the network's attack surface has expanded, requiring robust security measures to protect data and ensure privacy.

Why Are We Still Using Thirty-Five-Year-Old LAN Design Thinking?

Since Kalpana invented LAN switches in 1989 (later purchased by Cisco), traditional switch manufacturers have focused on switch capabilities. Over the next 15 years, most devices connected to the network were computers, printers, and Wi-Fi access points. Given endpoint characteristics, the focus was on switch capabilities without considering the endpoints being deployed. The primary consideration was delivering greater bandwidth to these endpoints. As a result, the industry evolved from using coax cable to Category 5E (or better) Ethernet cabling to support higher bandwidth delivery to the IP endpoint, regardless of the endpoint's bandwidth needs.

Ethernet was invented by Robert (Bob) Metcalfe, a computer scientist and engineer, while he was working at the Xerox Palo Alto Research Center (PARC) in the early 1970s. Metcalfe, along with his colleague David Boggs, developed Ethernet to enable computers to communicate with each other over a network using a common protocol. The key innovation was the use of a coaxial cable to transmit data packets in a local area network (LAN) environment.

Over the past twenty years, a greater number and a more diverse set of devices have been put on the LAN. However, LAN design methodology is still based on switch capabilities and not on the endpoint's requirements, resulting in significant ROI challenges for the business.

Like in many other industries, disruptive innovations are rarely introduced once the sector is monopolized or the largest players have invested significantly in the status quo. Consider Kodak, whose engineer invented the first digital camera. Kodak's leadership did not proceed with the invention because a significant amount of their profits came from film sales. Consider General Motors, who had a chance to be a leader in electric vehicles. General Motors embarked on an electric car pilot project in the 1970s, culminating in the creation of the Electrovair and Electrovair II. Several theories and speculations in the 2006 documentary "Who Killed the Electric Car?" suggest that oil companies, car manufacturers, and the federal government were interested in killing electric cars to protect the existing automotive and fossil fuel industries. It is speculated that these forces influenced General Motors' decision to end the EV1 program, maintaining the market's reliance on fossil fuels. GM had a chance to disrupt the auto industry but did not. Years later, social media allowed Elon Musk, who had no legacy challenges to consider and a blank sheet of paper, to disrupt the automotive industry and become the market leader in electric vehicles. Today, legacy car manufacturers rush to invest in electric vehicle development to mitigate the market share taken by Tesla.

Traditional network switch manufacturers, including those on the Gartner® Magic Quadrant™ for Wired and Wireless LAN Infrastructure, have significant legacy investments to protect. Their approach to network switch development is heavily influenced by original LAN design thinking and protecting legacy investments. As the number and variety of endpoints added to networks increased, network strategies came from the initial network paradigms established over 35 years ago. As a result of today's unique landscape, these outdated network design methodologies introduce greater complexity, higher costs, and a greater dependency on experts to solve problems and maintain networks. Despite these efforts, many reports highlight the increase in security breaches.

Network Vulnerability & Security Risks

Every day, we hear about a major security breach, and many reports provide detailed analyses of the trends, causes, and impacts. Here are some of the most notable reports and their key findings:

- The 2024 Verizon Data Breach Investigations Report, which analyzed data breach trends and security incidents across various industries, found increased frequency and sophistication of network breaches. Attackers' most common methods include phishing, ransomware, and credential theft. The industry's most targeted sectors include healthcare, finance, and public organizations. Many breaches involve human factors, such as misconfigured systems and employee mistakes.¹²
- An IBM report examines the financial impact of data breaches on organizations. The average cost of a data breach has reached \$4.88 million, a 10% increase from the previous year, underscoring the growing financial impact of cybersecurity failures. The report identifies compromised credentials, cloud misconfigurations, and third-party vulnerabilities as prevalent causes of breaches.¹³
- Cisco's Annual Cybersecurity Reports indicate increased frequency and sophistication of cyber-attacks, including network breaches. Ransomware attacks have become more targeted and destructive. Many organizations experience significant security gaps due to outdated infrastructure and inadequate security practices.¹⁴



There is a consistent increase in the number of network breaches year over year. Attacks are becoming more sophisticated, often involving multiple stages and advanced techniques. Human error, including misconfigurations and phishing attacks, remains a major factor in breaches. The financial impact of breaches is significant and growing, with substantial detection, response, and recovery costs. These reports collectively underscore the importance of robust cybersecurity measures, continuous monitoring, and employee training to mitigate the risk of network breaches. The ever-increasing attack plane for cyber-attacks means approaching network design with new principles is necessary to secure your network infrastructure. To this end, Modern LAN principles provide essential guidance on the private separation of data to allow for more robust security. Through these principles, we are challenged to consider the requirements of the endpoints themselves before beginning the network design – so we can build a purpose-built network.

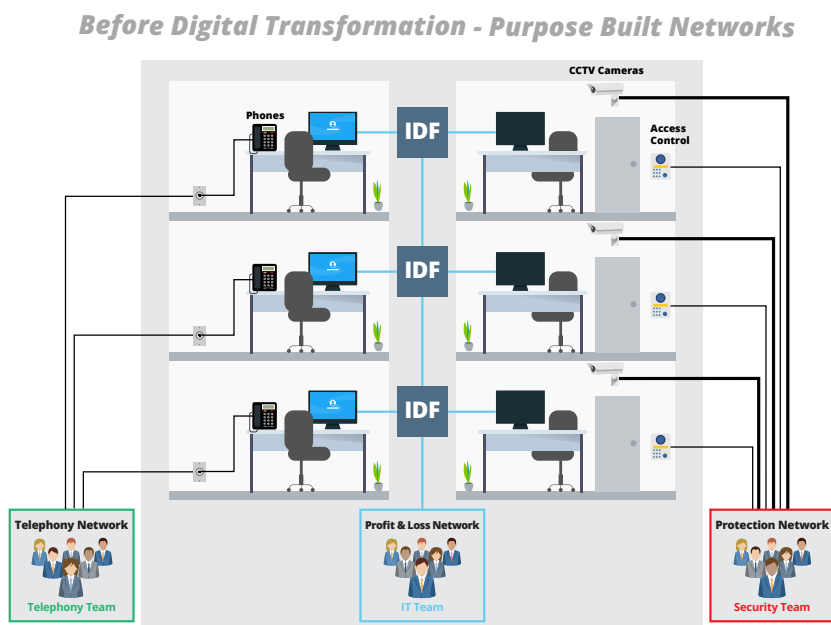
Modern LAN Design for Better Digital Transformation Outcomes

In 2019, Frost & Sullivan published the [Modern LAN Principles report](#). This report provides guidance on modern network design principles that support the deployment of modern IP devices and the digital transformation of businesses.

Albert Einstein once said “You can’t solve a problem with the same kind of thinking that created the problem,” and defined insanity as “doing the same thing over and over again and expecting different results.”

Modern LAN Principles emphasize beginning with endpoint requirements, understanding their impact on the network, and their bandwidth and power requirements. This may feel foreign, given that it is the opposite of conventional thinking, where network switch capabilities are the focus vs. focusing on the endpoints. A large percentage of IP endpoints on a typical LAN require less than 100 Mbps of bandwidth to operate effectively. Most devices, such as VoIP phones, IP cameras (especially at lower resolutions), printers, and IoT devices, have low bandwidth needs compared to data-intensive devices, such as Wi-Fi access points, which support several users and devices. Therefore, providing network infrastructure and PoE capabilities to support Gigabit+ speeds is unnecessary when most connected devices require less than 100Mbps.

By focusing on endpoint requirements, network planners realize that many cable infrastructures can effectively support these new IP devices' bandwidth and power requirements. For example, an organization with its core IT network supporting business requirements, a separate infrastructure supporting its legacy phones, and another supporting its legacy CCTV cameras and access control devices. These infrastructures were purpose-built for the endpoints and applications they enable. In addition, the proven and reliable coax and single-pair UPT cable infrastructures have a point-to-point topology. Every endpoint has a dedicated physical cable supporting its bandwidth and power needs. This network topology improves reliability, enhances security, and simplifies network management. Unfortunately, several traditional switch manufacturers do not offer PoE network innovations that can leverage these cable types due to the conflict-of-interest reasons mentioned earlier.



As noted in Frost & Sullivan's Modern LAN whitepaper, some smaller providers, such as NVT Phybridge, have introduced modern PoE network innovations that overcome cable type (CAT5 or better) and distance limitations (100m or 328ft) of standard switches. These innovations can deliver power and Ethernet over different cable types, including coax, single-pair UTP, 2-wire, and 2/4-pair UTP with extended reach capabilities. For years, organizations, including the most powerful federal agency in the world, the leader in space research, and thousands of global institutions, have leveraged Modern LAN principles and PoE innovations to eliminate LAN barriers and concerns.

Given the power and influence of traditional switch manufacturers and network providers, it may take time to identify the leaders in PoE innovations. When speaking with network providers and planning a digital transformation project, use objectives and desired outcomes to guide the conversation and the strategy. Organizations may need to push back against traditional strategies that create high costs, complexity, and risk but provide high revenues and margins for the network provider. Construct a purpose-built network that will result in the best outcomes considering the deployed endpoints rather than taking the "one-size-fits-all" approach. Free yourself of the complexity, high costs, and security concerns associated with traditional and outdated LAN design thinking.

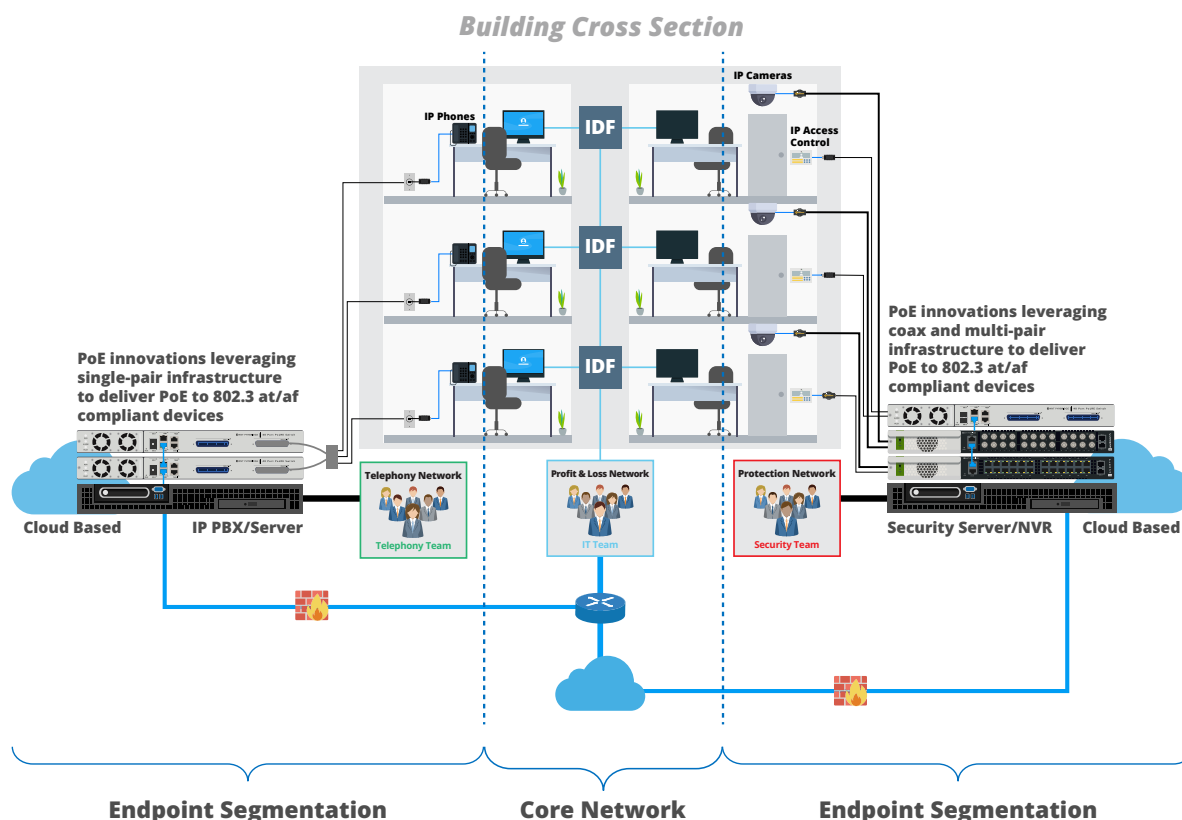
Implementing A Purpose-Built and Modern LAN Design

To illustrate modern network design, reference the building cross-section below with multiple floors, highlighting three distinct networks.

The core traditional network has switches in multiple IDF closets, which are necessary due to switch reach limitations. Traditional endpoints such as computers, Wi-Fi access points, and printers are connected from these IDF closets. This core network enables end users to leverage business data to create the desired business outcomes.

There are two complementary IP sub-networks. Each complimentary network leverages the existing, purpose-built, point-to-point topology with PoE innovations to enable supporting endpoints that enhance corporate communications and security capabilities. The telephony/unified communications network is on the left. PoE switches leveraging single-pair UTP cabling are all in a single MDF closet, leveraging existing assets such as rack space, power source, and backup power capabilities. The physical security network on the right is designed to protect people and assets. It leverages existing coax or multi-pair UTP cabling to enable physical security endpoints. Like the voice network on the left, it is purpose-built with a point-to-point topology.

This network strategy allows organizations to physically segment their supportive endpoints, including bandwidth and power requirements, which helps protect the uptime and performance of the core business network that drives business outcomes for the business. Physical segmentation is much more effective than virtual segmentation using VLAN methods. Traditional VLAN methods are more complex to manage and do not address power requirements for the endpoints.

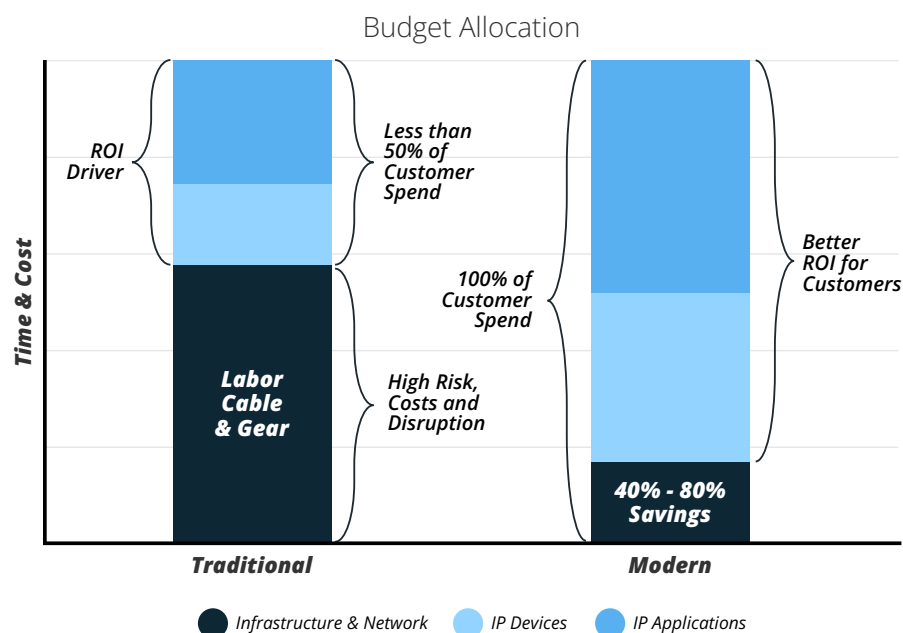


Benefits of Modern LAN Principles

There are many benefits of leveraging Modern LAN Principles and new PoE innovations.

Lower Network Readiness Costs

For retrofit environments, the ability to leverage existing wiring assets and network infrastructure reduces the costs of establishing a PoE network. For new environments, the extended reach and potentially lower cost wiring (using single pair for low power and bandwidth endpoints) eliminate the need for more IDF closets and expensive cable infrastructure. Organizations have used these strategies to achieve up to 80% cost savings to establish a PoE network for IP devices. In addition to lower deployment costs, the total cost of ownership is lower, given the simplicity of ongoing network management. For new environments, extended reach capabilities and cable type options allow organizations to eliminate IDF closet requirements and costs.



Enhanced Network Security

Physically separating IP devices from the core business network provides the highest form of security. Segmenting the supporting IP endpoints from the core network can better support organizations' security objectives. If necessary, organizations can securely converge the supportive and core networks using a single wire and a firewall for additional security.

Better Return on Investment

As highlighted in Frost & Sullivan's Modern LAN Whitepaper, the traditional network approach to digital transformation often leads to cost overruns, complexity, and network reliability concerns. There are typically three major components to an IP upgrade; IP endpoints, applications and application adoption, and LAN infrastructure that connects the endpoints to the application. Modern LAN Principles and modern PoE innovations will reduce overall network costs, allowing organizations to allocate more digital transformation budgets to the ROI drivers—the endpoints, applications, and application adoption.



Network Futureproofing

Given the increasing bandwidth requirements, core LAN switch requirements change every five years. Organizations will significantly reduce future costs and complexities when completing core network refresh requirements by segmenting IP endpoints that do not require and will never require more than 100Mbps on a separate PoE backbone.

Network Simplicity

Applying Modern LAN Principles and physically segmenting supportive IP endpoints on their own sub-network will reduce deployment and ongoing management complexity. These subnetworks can be converged with a single cable, or kept completely separate from the core business network. IT teams have complete control, simplifying management while greatly reducing stress levels .

Environmentally Responsible Modernization

In addition to all the above benefits, organizations will reduce the environmental impact of their digital transformation project by reducing cabling and other electronic waste. Leverage existing cabling and network infrastructure assets in a retrofit project, significantly reduce IDF closet requirements in new environments, and use more efficient cabling infrastructure to enable endpoints. For example, use existing single-pair UTP cabling to support an IP phone deployment instead of laying new CAT5/6 cable with four pairs of UTP cable to support one phone. For new deployment, organizations can support up to four IP phones with a single CAT5/6 cable by using modern PoE innovations.

Tested and Proven Strategies

Do these outcomes sound too good to be true? Visit www.modernLAN.org to learn more about modern network design principles, and download the Frost & Sullivan Modern LAN Whitepaper to read about successful implementations. Visit www.nvtphybridge.com to view modern PoE innovations that enable Modern LAN Principles and create better digital transformation outcomes for organizations worldwide. [Download our free Digital Transformation Sanity Checklist](#) to help you make an informed networking decision. Maximize your digital transformation ROI while building a secure and robust local area network that fits your needs.

Avoid Potential Conflict of Interest

[Download "Are Your Technology Providers Keeping You in The Dark?"](#) to learn how to avoid the potential conflict of interest that may negatively impact your digital transformation ROI.

About Us – Our Mission

NVT Phybridge is a global leader in long reach Power over Ethernet solutions. Our mission is to help organizations maximize their IoT return on investment by providing high-quality PoE solutions that are robust, secure, and simple-to-implement. Our award-winning CHARIoT series of long reach PoE switches and extenders help organizations deploy the latest IP and IoT technologies, over any new or existing network infrastructure, without high costs, complexity, or disruption!



3457 Superior Court, Unit 3
Oakville, ON
L6L 0C4



888.901.3633



www.nvtphybridge.com



Bibliography

Cisco. (2024). Cisco Cybersecurity Report Series. Retrieved from Cisco Systems Inc.:

https://www.cisco.com/c/en_ca/products/security/security-reports.html

Davenport, T., & Westerman, G. (2018, March 9). Why So Many High-Profile Digital Transformations Fail. Retrieved from Harvard Business Review: <https://hbr.org/2018/03/why-so-many-high-profile-digital-transformations-fail>

Devo Technology Inc. (2019, July 29). Ponemon Institute and Devo Technology Study Reveals 65% of Cybersecurity Analysts Consider Quitting Due to Burnout, Lack of Visibility. Retrieved from Devo Technology: <https://www.devo.com/company/newsroom/ponemon-institute-and-devo-technology-study-reveals-65-of-cybersecurity-analysts-consider-quitting-due-to-burnout-lack-of-visibility/>

Forth, P., Reichert, T., Laubier, R. d., & Chakraborty, S. (2020, October 29). Flipping the Odds of Digital Transformation Success. Retrieved from <https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation>

Gartner, Inc. (2024). Forward-thinking insights that help infrastructure and IT operations (I&O) executives reinvent how they deliver value for the business. Retrieved from Gartner, Inc.: <https://www.gartner.com/en/infrastructure-and-it-operations-leaders/role/infrastructure-operations-leaders>

Gartner, Inc. (2024, January 25). Gartner Survey Shows That Leading Transformation Is the Top Priority for CFOs in 2024. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2024-01-25-gartner-survey-shows-that-leading-ransformation-is-the-top-priority-for-cfos-in-2024>

Geitz, M. (2024, February 27). Key Insights From The Digital Transformation Forrester Wave™ Q4, 2023. Retrieved from Forrester Research, Inc.: <https://www.forrester.com/report/key-insights-from-the-digital-transformation-forrester-wave-tm-q4-2023/RES180597>

IBM. (2023). Cost of a Data Breach Report 2023. Retrieved from IBM: <https://www.ibm.com/reports/data-breach>

McKinsey & Company. (2018, October 29). Unlocking success in digital transformations. Retrieved from McKinsey & Company: <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations>

Popova, E. (2019, February 6). Modern LAN: Putting it All Together with Modern LAN Principles. Retrieved from Frost & Sullivan: <https://www.frost.com/frost-perspectives/modern-lan-putting-it-all-together-with-modern-lan-principles/>

PwC. (2017). A decade of digital: Keeping pace with transformation. Retrieved from PwC: <https://www.pwc.com/ee/et/publications/pub/pwc-digital-iq-report.pdf>

Verizon. (2024). 2024 Data Breach Investigations Report. Retrieved from Verizon: <https://www.verizon.com/business/resources/reports/dbir/>