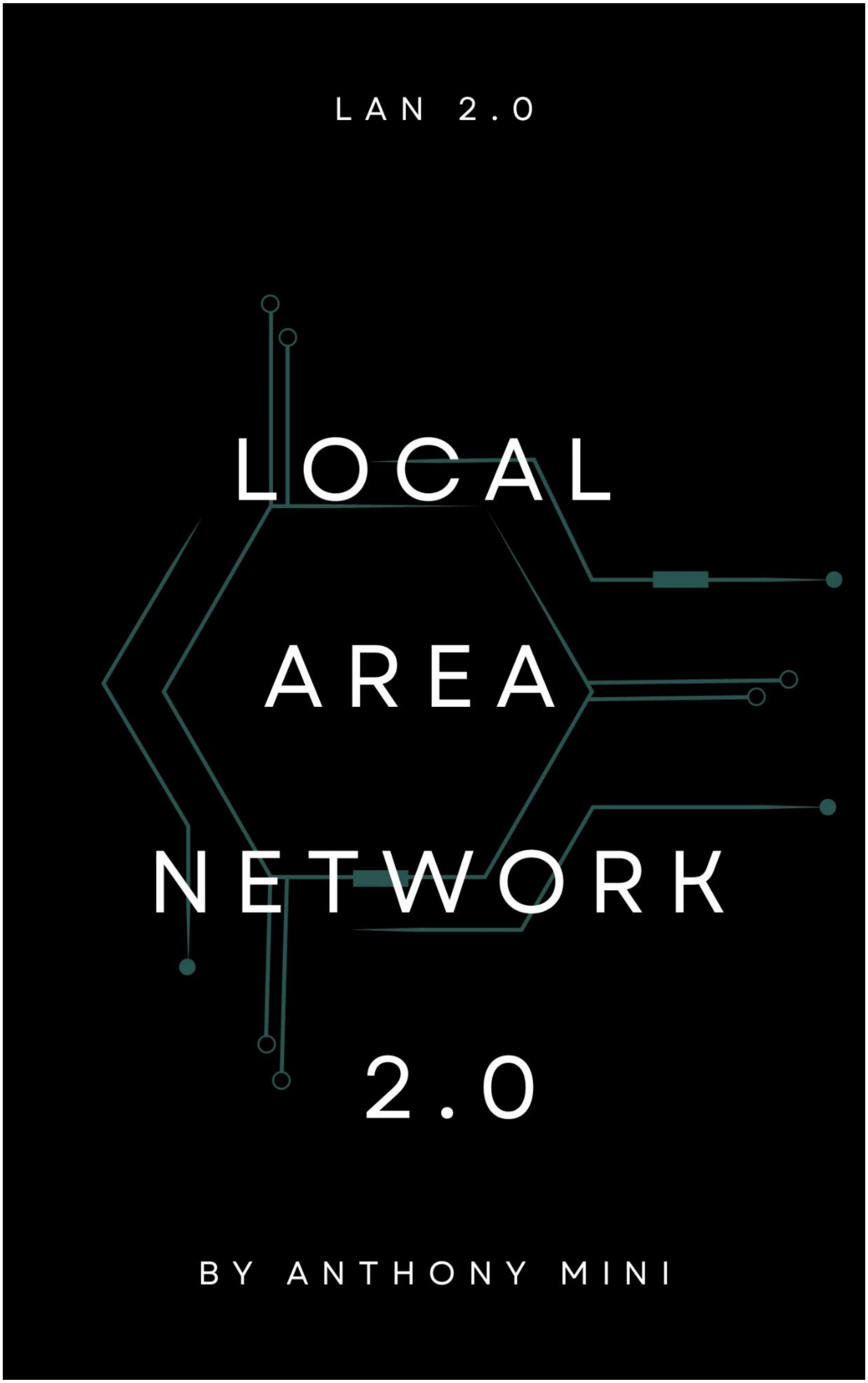


LAN 2.0

LOCAL AREA NETWORK 2.0

BY ANTHONY MINI

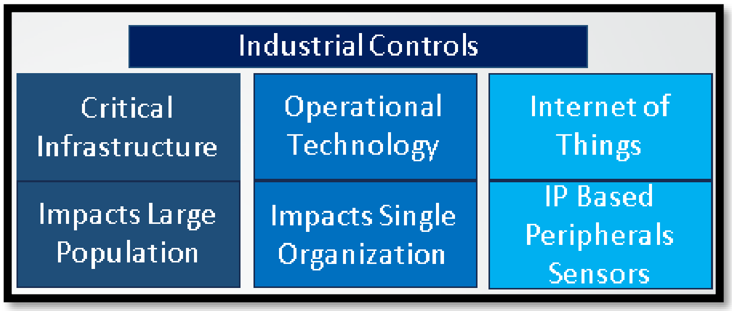
Introduction

From its inception, the internet has undergone numerous changes and advancements, transforming the way we communicate, learn, and do business. However, one aspect that has remained relatively unchanged is the Local Area Network (LAN)—also known as Personal Area Network (PAN) and Campus Area Network (CAN)—the private IP space that runs at the core of digital enterprise. However, with the introduction of cloud technology and the convergence of non-traditional networked devices, the LAN is undergoing a significant migration that is redefining its role in the ever-evolving cyber landscape. This transformation has given rise to the concept of "LAN 2.0," ushering in a new era of connectivity and security designs. In this white paper, we will explore the components of LAN 2.0, the factors driving its evolution, and the potential security concerns that come with this new frontier. From the increasing integration of Operational Technology (OT) and Internet of Things (IoT) devices to the pressing need for collaboration and best practices, let's delve into the captivating world of LAN 2.0.

The concept of the world wide web has morphed at a hyper rate of transformation throughout its existence. It has been classified into different stages such as the read-only Web 1.0, the more interactive Web 2.0, and the loosely defined decentralized Web 3.0. Currently, there is an ongoing development of the underground and ambitious idea of Web 4.0. However, while the internet has experienced this evolution, the private IP space has remained relatively unchanged. Similarly, the emergence of cloud technology and the convergence of non-traditional networked devices has morphed the LAN into a less static environment.

Various organizations have adopted different approaches when it comes to implementing Wide Area Network (WAN) frameworks, hybrid cloud models, and merging their IoT… all of which has transformed the traditional LAN drastically enough to redefine how we conceptualize and protect it.

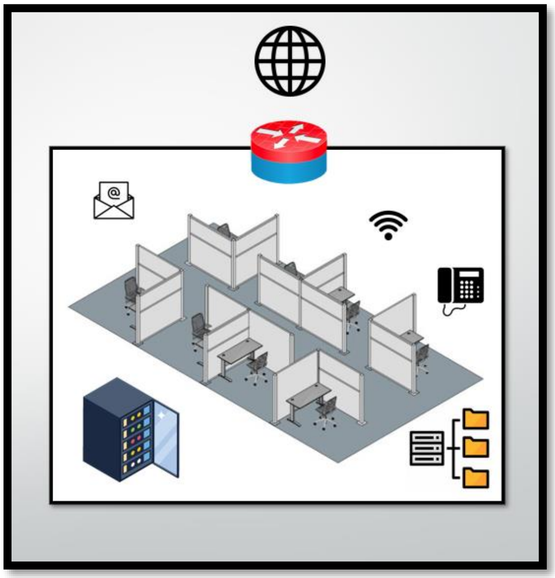
Definitions



Industrial Controls		
Critical Infrastructure	Operational Technology	Internet of Things
Impacts Large Population	Impacts Single Organization	IP Based Peripherals Sensors

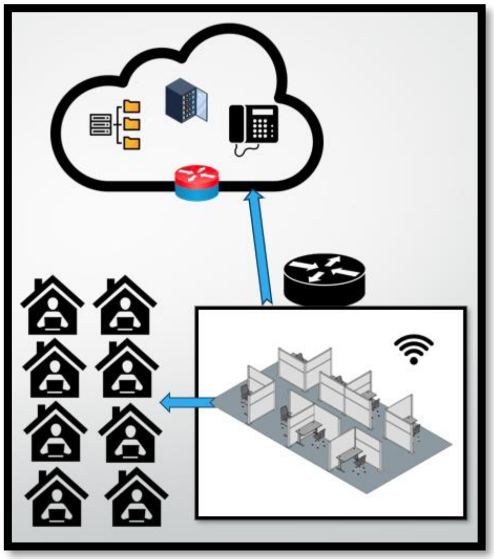
First, to provide clarity, consistency, and perspective to the theories, we define "Critical Infrastructure" (CI) as vital assets of a WAN that are essential to the functionality of a region or nation. "OT" is defined as assets on a LAN that are imperative for the operations of a specific organization. Meanwhile, IoT includes LAN and WAN peripheral assets that are not crucial to an organization but are still connected to IP-based networks. These definitions are dynamic based on the organizations. For example, a surveillance camera system may not be crucial to a marketing company (defined as IoT), but its outage could affect the safety of prison (defined as OT) facility operations.

LAN Migration(s)



During the early 2000s, those of us who were fortunate enough to work as network administrators had a deep appreciation for the static and straightforward model of the LAN. This fortified structure made it easy for us to understand the edges, boundaries, and location of our valuable assets.

We had a thorough understanding of the North/South and East/West traffic flow and were able to effectively segment our networks, managing access and objects with Access Control Lists (ACL) and Lightweight Directory Access Protocol (LDAP) system. It truly was the "good ol' days."

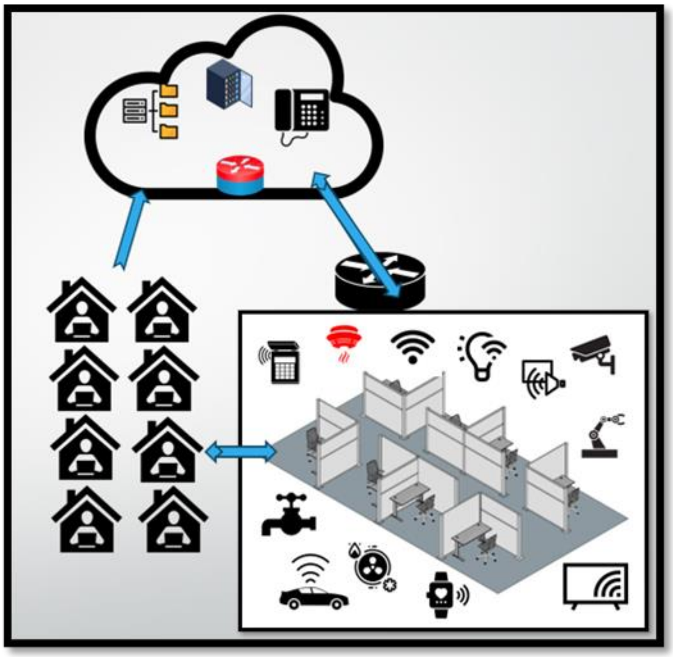


The first contributing factor to changes within the LAN is the great migration to the cloud. The migration to the cloud was activated with “cloud first” strategies and data center consolidation efforts like the US Federal Data Center Consolidation Initiative. Then, COVID put the migration strategies into hyper speed.

During COVID, many organizations were forced to migrate quickly to maintain operations with Work from Home (WFH) technologies, then adapted security models such as Secure Access Service Edge (SASE) and Zero Trust after the fact. Many of these terms got blurred with vendor marketing campaigns and proprietary technologies, but SASE essentially extended the LAN into a WAN, and Zero Trust shortened the boundaries to the endpoints. The result was data computing outside the organization’s traditional security stack in their “on-prem” data center to more distributed home offices utilizing VPNs and Software as a Services (SaaS) platforms.

Next, the convergence of OT and IoT devices connecting to the network is the second contributing factor to changes within the LAN. In recent years, OT and IoT have become increasingly integrated within traditional IT enterprises, resulting in significant changes to data and protocols transmitted over private IP networks. Terms such as CI and OT are used to describe industrial systems that fall under the 16 CI sectors designated by the Department of Homeland Security (DHS). These systems are considered vital to the United States, and their incapacitation or destruction would have a detrimental impact on national security, economic security, public health, or safety.

Previously, many OT and IoT systems were isolated on analog networks. However, as companies adopt new systems, they are increasingly transitioning to IP-based systems. Vendors now primarily only offer IP-based systems, and it is too costly to maintain a separate network for OT/IoT systems. As a result, communication protocols such as Modbus, DNP3, PROFIBUS, PROFINET, BACnet, DMX, and others are now operating on LANs in the form of audiovisual systems, payment systems, kiosks, water systems, HVAC, closed-circuit television, surveillance and intrusion detection systems, paging systems, building management systems, industrial control systems, and supervisory control and data. The emergence of IoT smart technologies has further contributed to the connection of devices such as Tesla cars, robots, and audiovisual systems to wireless networks.



Cybersecurity Concerns

Cybersecurity concerns regarding OT/IoT have become a pressing issue. These systems are prime targets for several reasons, one of which is their impact on the physical world. This means that the risks involved are on a larger scale compared to information-only data systems. The potential consequences include loss of life, ecological harm, theft of intellectual property, damage to a brand's reputation, and significant financial losses. Moreover, OT systems are often used as a starting point to gain access to enterprise networks, allowing attackers to pivot and exploit other data systems. This was first demonstrated during the well-known 2013 Target breach, where HVAC vendor access was leveraged to access Point of Sale (PoS) devices and used to steal credit card information.

The emergence of ransomware in LAN 2.0 has also contributed to the rise of cybersecurity concerns. Threat actors have shifted their focus from organizations with desirable assets, such as Protected Health Information (PHI), Personally Identifiable Information (PII), Proprietary Information (PI), and Classified Information, to ANY networked systems that can be taken offline. In such cases, the attackers demand ransom in exchange for the decryption keys to bring the systems back online. Furthermore, there is a risk of double extortion, where the threat actors not only hold the system hostage but also threaten to release stolen protected data if their demands are not met.

Another factor contributing to the increasing vulnerability of OT/IoT systems is the rapidly expanding attack surface with the rise of the IoT industry, which is determined to deliver a multitude of devices to consumers in a market largely driven by affordability and user-friendliness. Threat actors are targeting IoT/OT systems because they are consistently online and can be used for purposes such as crypto mining or gaining persistent access.

The differences between the development and implementation of cybersecurity in the OT and IT realms need standardization. Despite the growing importance of securing OT systems, it is apparent that OT cybersecurity is markedly behind IT security in terms of organizational development, funding, available tools, and resources. IoT/OT components were not designed with security considerations in mind, resulting in outdated systems, protocols, and priorities. This lack of foresight has left these systems vulnerable to newer cyber threats. While the IT realm has largely adopted the standardized TCP/IP protocol, the OT domain is lacking such uniformity. These differing protocols often lack compatibility with each other and do not align with the common protocols used in IT-based security tools.

Overall, the concerns surrounding IoT/OT convergence are significant and demand immediate attention. It is essential that the IoT/OT realm catches up to the level of cybersecurity preparedness that the IT realm has achieved. It is imperative for organizations to invest in the necessary resources and tools to secure their OT systems and bridge the gap between IT and OT cybersecurity. Without addressing these concerns, the risk of cyber attacks on CI and industrial control systems will continue to grow.

<u>Human Layer</u>

One underreported yet crucial issue surrounding LAN 2.0 systems is that of human layer and ownership. In some organizations, the OT systems were typically owned and managed separately by each individual department, rather than being under the control of the IT department. This often resulted in a focus on functionality over security in the design and acquisition of systems. In other organizations, the responsibility fell on the IT department to design and acquire technology, despite the IT department lacking expertise in these specific technologies and protocols.

LAN 2.0 is crucial for ownership to align with the organization's cybersecurity risk management strategy. This requires a collaborative approach between mission owners and cybersecurity teams. It is important to recognize that individuals solely specialized in either OT or IT cannot fulfill all the security requirements on their own. To effectively reduce enterprise risk and safeguard the entire cyber domain, it is crucial to develop a strategic staffing plan that integrates IT and OT duties into the workforce development program. This will promote a more cohesive and comprehensive approach to cybersecurity within the organization.

LAN 2.0 will require network administrators to shift from technical knowledge of traditional on-premises system administration to vendor management subject matter expertise (SMEs) of Service Level Agreements, Scopes of Works, etc. In many cases, network admins will need to identify what level of telemetry logs they have access to with their SaaS vendors, and they will need to justify the expense of expensive subscriptions for advanced logs.

Best Practices

Now that we have a better understanding of LAN 2.0 and its associated cybersecurity concerns, it is imperative to establish effective best practices for managing this new domain. In many cases, this means going back to basics. Here are 12 recommendations and how they are different from the traditional LAN 1.0 methodologies.

1. **Asset Management:** This will be increasingly more difficult with the distribution and diversity of technologies. This is the most important aspect of cybersecurity LAN 2.0. By improving organizations' visibility and control over their assets, potential vulnerabilities in the infrastructure can be identified and risk managed.
2. **Consolidation:** Organizations need to converge the IT and IoT/OT security efforts from user awareness to vulnerability management and IR playbooks.
3. **Patch Management:** With the increase in attack surface, and the lack of holistic patching tools, it will take intentional effort to know all the IT, IoT, OT systems and their patching status. Patching OT systems will be even more risky to avoid hindering production.
4. **Enterprise Monitoring**: Research and design the best monitoring approach for your operations. Understand when to leverage Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Extended Detection and Response (XDR), and Security Information and Event Management (SIEM) technologies based on the business operations and enterprise architecture. OT specific network monitoring tools, such as the free NSA tool Grass Marlin and vulnerability scanning tools that are less intrusive to OT/IoT devices.

5. **Scanning:** Active scanning can break your IoT/OT equipment. You will need a customizable scan approach and adjust scan intensities and minimizing disruptions to critical operations. Utilize both agentless and agent-based vulnerability scanning technologies for flexibility in scanning various devices.
6. **Protection:** Incorporate EDR capabilities. This takes a careful effort to avoid breaking your environment. You may need to test the best EDR for your needs, and you may need to mix a combination of EDR technologies.
7. **Access Management:** Authentication controls will be different compared to the LAN 1.0 LDAP, but new technologies have emerged to facilitate the administration. Controlling hybrid cloud access will require the use of Single Sign On (SSO), Cloud Access Security Broker (CASB), and password managers for systems that do not yet integrate with technologies such as Security Assertion Markup Language (SAML).

8. **Multifactor Authentication:** This may be bolted on until these technologies are built with more capabilities.

9. **Physical Security:** Locking racks, disabling ports on kiosks, using camera covers, and USB blockers should also be used.

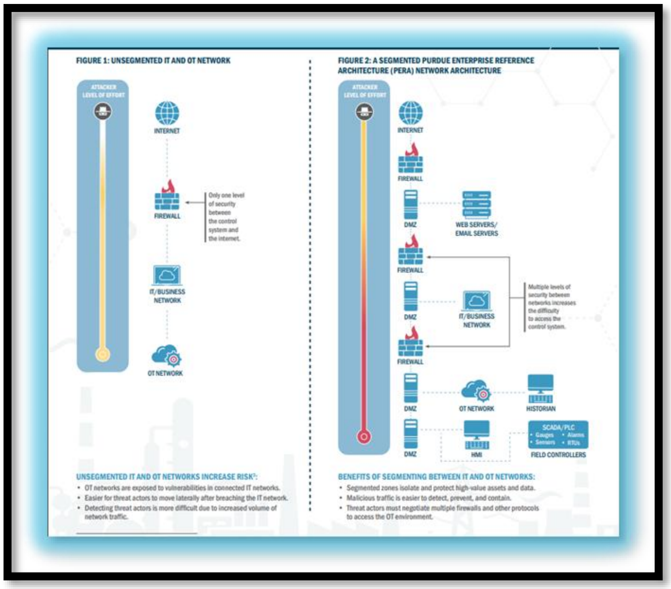


FIGURE 1: UNSEGMENTED IT AND OT NETWORK

ATTACKER LEVEL OF EFFORT
INTERNET
FIREWALL
Only one level of security between the control system and the internet.
IT/BUSINESS NETWORK
OT NETWORK

UNSEGMENTED IT AND OT NETWORKS INCREASE RISK[3]:

- OT networks are exposed to vulnerabilities in connected IT networks.
- Easier for threat actors to move laterally after breaching the IT network.
- Detecting threat actors is more difficult due to increased volume of network traffic.

FIGURE 2: A SEGMENTED PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA) NETWORK ARCHITECTURE

BENEFITS OF SEGMENTING BETWEEN IT AND OT NETWORKS:

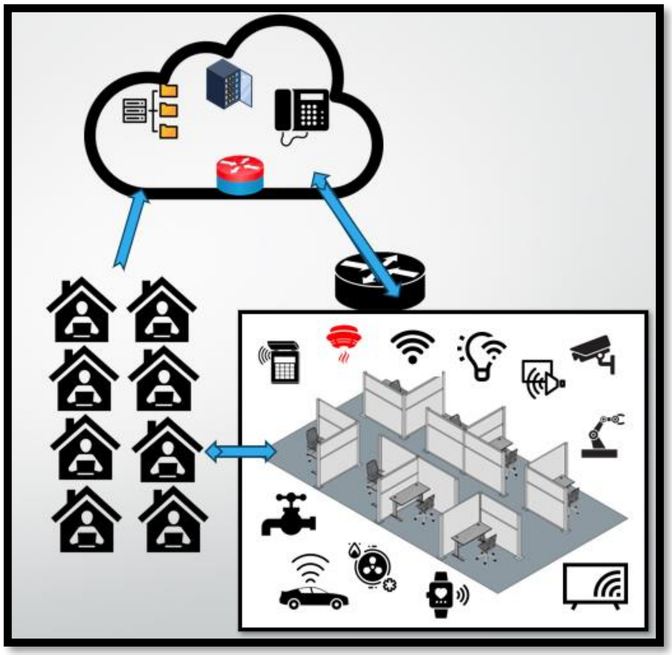
- Segmented zones isolate and protect high-value assets and data.
- Malicious traffic is easier to detect, prevent, and contain.
- Threat actors must negotiate multiple firewalls and other protocols to access the OT environment.

10. **Harden Key Terrain**: IoT/OT devices have a way of opening ports and protocols to your networks as vendors troubleshoot getting these things to operate. You will need to constantly revisit disabling unnecessary ports, protocols, and features.

11. **Network Segmentation:** A VLAN design will be absolutely critical.

12. **Secure Communications:** Utilizing a device that is IoT SAFE-compatible, one can establish a secure connection to the cloud through a mutually authenticated Transport Layer Security (TLS) session, known as Zero Touch Provisioning.

Conclusion



The LAN has traditionally been relatively static and unchanged throughout the evolution of the internet. However, with the emergence of cloud technology and the convergence of non-traditional networked devices, the LAN is undergoing a great migration and becoming significantly different from its previous form. This transformation has led to the development of LAN 2.0, with the integration of OT and IoT devices, along with challenges such as cybersecurity risks and ownership. To effectively manage these changes, it is crucial for organizations to prioritize collaboration and joint education between IT and OT departments, establish asset management protocols, and implement networking best practices and zero-trust security principles. As LAN 2.0 continues to evolve, it is imperative for organizations to adapt and innovate to secure their networks and protect against potential cyber threats.