

WIRED AND WIRELESS NETWORKS: A COMPARATIVE STUDY

ISHARA BARHOSON GALADIMA¹, BENJAMIN, UBOKOBONG EFFIONG²

¹Dept. of computer science, Nuhu Bamalli Polytechnic, Zaria

²Dept. of computer science, Akwa Ibom State Polytechnic

Email: isharag873@gmail.com¹, ubokobong.benjamin@akwaibompoly.edu.ng²

D.O.I: 10.5281/zenodo.15545915

ARTICLE INFORMATION

Received: 27th Feb 2025

Accepted: 31ST March, 2025

Published: 30th April, 2025

KEYWORDS: Wired, Wireless
Networks, Comparative Study

JOURNAL URL:
<https://ijois.com/index.php/jobpef>

PUBLISHER: Empirical Studies and
Communication (A Research
Center)
Website: www.cescd.com.ng

This work is licensed under the Creative
Commons Attribution International
License (CC BY 4.0).



Open Access

<http://creativecommons.org/licenses/by/4.0/>

ABSTRACT

This paper examines the differences between wired and wireless networks, especially in educational settings. It explains how each type of network works, their advantages, and their disadvantages. Wired networks are often chosen for their fast speeds, strong security, and dependable connections, making them ideal for places that need stable internet. Wireless networks, however, are easier to install, allow users to move around freely, and can be expanded quickly, which is useful in classrooms that need flexibility. The study compares both types of networks in terms of speed, security, cost, and how easy they are to use. It also looks at how these networks support online learning and digital tools. The aim is to help teachers, school staff, and IT professionals pick the right network to improve learning and connectivity.

Keywords: Artificial Intelligence (AI), Workplace Activities, Local Government Administration, Tracking Systems

Keywords: Wired, Wireless Networks, Comparative Study

INTRODUCTION

In the digital age, computer networks have become foundational to global communication, enabling the seamless exchange of information and collaboration across multiple domains (Kurose & Ross, 2020; Stallings, 2017). As the Internet continues to expand, interconnecting billions of devices, it supports a wide spectrum of services—from social interaction and entertainment to enterprise operations and critical infrastructure. This growing dependence on interconnected systems underscores the importance of robust, scalable, and efficient networking infrastructures (Stallings, 2017).

Wired networks, which rely on physical transmission media such as copper cables and fiber optics, have traditionally dominated network infrastructures due to their high throughput, low latency, and consistent performance. These characteristics make them especially suitable for environments where reliability and speed are paramount (Tanenbaum & Wetherall, 2014). On the other hand, wireless networks leverage radio frequencies or infrared signals to enable device communication without physical connections. Their ease of deployment and support for user mobility have made them essential in dynamic environments and mobile computing scenarios (Goldsmith, 2021). However, wireless systems often face challenges such as signal interference, attenuation, and inconsistent data transmission rates due to their dependence on atmospheric and environmental conditions (Goldsmith, 2021). Technologies like Wi-Fi and cellular networks highlight the widespread adoption and versatility of wireless communication, especially in the context of mobile devices and Internet of Things (IoT) ecosystems (Kurose & Ross, 2020; Stallings, 2017).

Despite technological advancements, each networking approach presents its own strengths and limitations. Wired solutions generally outperform in terms of stability, security, and bandwidth, while wireless options offer greater flexibility, ease of installation, and scalability (Tanenbaum & Wetherall, 2014; Goldsmith, 2021). Consequently, selecting between these two paradigms often requires careful consideration of contextual needs and operational constraints (Stallings, 2017).

This study offers a detailed comparative assessment of wired and wireless networks, focusing on essential performance indicators such as bandwidth, latency, cost, and security. The objective is to guide stakeholders in choosing or combining network types effectively to meet the requirements of various use cases and emerging technological trends.

History of Computer Networks

The progression of computer networking has been a cornerstone in the advancement of communication and information technology. From initial experimental setups to today's intricate global systems, networks have fundamentally changed how data is exchanged and accessed.

Networking concepts began to take shape in the late 1950s and early 1960s, primarily to connect large mainframe computers for resource sharing. A significant point was the **ARPANET**, initiated in 1969 by the U.S. Department of Defense, which introduced packet-switching, a method that breaks data into packets for efficient transmission. This innovation laid the foundation for the protocols that underpin the modern Internet.

In the 1980s, Ethernet technology became the dominant standard for local area networks (LANs), enabling faster and more reliable communication within confined spaces like offices and campuses. The IEEE 802 standards formalized these protocols, facilitating widespread adoption. Simultaneously, the TCP/IP protocol suite was developed and standardized, providing a universal language for diverse networks to interconnect seamlessly. 1990s witnessed the explosive expansion of the Internet, largely driven by the invention of the World Wide Web by Tim Berners-Lee in 1989. This innovation made the

Internet accessible and useful to the general public. Around the same time, wireless networking technologies such as Wi-Fi (IEEE 802.11) emerged, allowing users to connect without physical cables and enhancing mobility.

Types and Characteristics of Networks

Networks can be categorized based on their size, function, and technology. Below are the primary types:

Local Area Network (LAN)

LANs link devices within a limited area such as a home, office, or school. They provide high-speed connections and low latency, ideal for sharing files, printers, and applications locally.

Wide Area Network (WAN)

WANs cover broad geographic regions, connecting multiple LANs across cities, countries, or continents. The Internet is the largest example of a WAN, utilizing various communication infrastructures like leased lines and satellites.

Metropolitan Area Network (MAN)

MANs serve larger areas than LANs but smaller than WANs, typically spanning cities or large campuses. They offer high-speed connectivity to support organizations like universities or municipal governments.

Concept of Wireless Networks

These networks transmit data through radio waves or infrared signals instead of cables. Examples include Wi-Fi for local wireless access, Bluetooth for short-range device communication, and cellular networks (4G/5G) for wide-area mobile connectivity.

Personal Area Network (PAN)

PANs are small networks centered around an individual's personal devices, such as smartphones, tablets, and wearables. They usually operate within a range of about 10 meters using technologies like Bluetooth.

Virtual Private Network (VPN)

VPNs establish encrypted tunnels over public networks, ensuring secure and private communication. They are widely used for remote access, data protection, and bypassing geographic restrictions.

Storage Area Network (SAN)

SANs are specialized networks designed to provide high-speed access to consolidated storage devices, commonly used in enterprise environments to manage large volumes of data efficiently.

Campus Area Network (CAN)

CANs connect multiple LANs within a limited geographic area such as a university or corporate campus, enabling resource sharing across buildings.

Overview of Wired Networks

A wired network refers to a system of interconnected devices that rely on physical cables, such as Ethernet, coaxial, or fiber optics, to transmit data. These networks are commonly used in environments

where high performance, reliability, and security are critical, such as offices, data centers, and industrial facilities (Tanenbaum & Wetherall, 2014). The rapid development of computer networks has introduced considerable challenges in designing systems that are both efficient and scalable while addressing real-world constraints. Although theoretical models in networking have advanced significantly, a gap persists between these models and their practical implementation, limiting the optimization of network performance in environments with dynamic traffic, constrained resources, and diverse service demands (Kurose & Ross, 2020). Innovative concepts such as Computing-Aware Networking (CAN) stress the importance of dynamically directing traffic to the most suitable service instances based on real-time computing and network resource availability. However, current solutions often struggle to balance computational loads effectively or adapt to the fluctuating conditions typical of edge computing infrastructures. This results in inefficient resource use, higher operational costs, and diminished user experience (Stallings, 2017; Tanenbaum & Wetherall, 2014).

Key attributes of wired Networks

- **Cables:** Wired networks use physical media like Ethernet cables for short distances or fiber optic cables for high-speed, long-distance communication.
- **Devices:** Routers, switches, hubs, and network interface cards (NICs) facilitate data transmission within the network.
- **Data Transmission:** Data is sent as electrical signals (Ethernet/coaxial) or light signals (fiber optics), offering stable and interference-free communication.

Advantages

1. **Performance:** Wired networks provide high bandwidth and low latency, making them suitable for tasks requiring consistent speed and reliability (Kurose & Ross, 2020).
2. **Reliability:** Physical connections are less prone to interference from environmental factors like weather or electromagnetic signals.
3. **Security:** Since access requires a direct physical connection, wired networks are inherently more secure than wireless ones (Stallings, 2017).

Disadvantages

1. **Cost and Installation Complexity:** Deploying a wired network involves higher costs due to cabling and infrastructure setup.
2. **Limited Mobility:** Devices are tethered to specific locations, reducing flexibility compared to wireless networks.

Applications

Wired networks are widely used in:

- **Data Centers:** For high-speed data processing and storage.
- **Corporate Offices:** To ensure secure and reliable communication.
- **Industrial Systems:** For automation processes requiring precision and stability.

Future Trends

Advancements like Power over Ethernet (PoE), which allows devices to be powered through Ethernet cables, and improvements in fiber optic technology continue to enhance the capabilities of wired networks (Goldsmith, 2021).

Overview of Wireless Networks

Wireless networks enable devices to communicate and exchange data without the need for physical cables, using radio waves or other wireless technologies. These networks have become essential in everyday life, providing mobility, flexibility, and easy scalability for both personal and business use (TutorialsPoint, 2025; Fortinet, 2025).

Key Characteristics

- **Wireless Communication:** Data is transmitted through radio frequency (RF) or infrared signals between devices such as routers, access points, and client devices (Ruckus Networks, 2025).
- **Mobility:** Wireless networks allow users to stay connected while moving within the network's coverage area, offering significant convenience.
- **Network Categories:** Wireless networks are classified based on their coverage area and function:
 - ❖ **Wireless Local Area Networks (WLANs):** Connect devices within limited spaces like homes or offices.
 - ❖ **Wireless Metropolitan Area Networks (WMANs):** Cover larger regions such as cities by linking multiple WLANs.
 - ❖ **Wireless Wide Area Networks (WWANs):** Span extensive areas by integrating several smaller networks (TutorialsPoint, 2021; Fortinet, 2025).

Benefits

1. **Simple Setup:** Wireless networks avoid the complexity of running cables, making installation quicker and easier.
2. **Flexibility:** Devices can connect from any location within the network's range without being physically connected.
3. **Easy Expansion:** Adding new devices is straightforward since there are no physical cabling constraints.
4. **Cost Savings:** Reduced need for wiring lowers both installation and maintenance expenses (TutorialsPoint, 2025; Ruckus Networks, 2025).

Limitations

1. **Variable Performance:** Wireless signals can be affected by interference from environmental factors or other electronic devices.

- 2. Security Risks: Wireless transmissions are more vulnerable to unauthorized access, necessitating strong encryption and security protocols (Fortinet, 2025).
- 3. Range Restrictions: The effective coverage area depends on signal strength and may require additional infrastructure for larger environments.

Comparative Table of Network Types Based on Key Metrics

Metric	Personal Area Network (PAN)	Local Area Network (LAN)	Metropolitan Area Network (MAN)	Wide Area Network (WAN)
Bandwidth/Speed	Low; suitable for small data transfers (e.g., Bluetooth)	High; supports fast data transfer within a limited area	Moderate; depends on infrastructure, typically slower than LAN	Variable; can range from moderate to high depending on the connection type (e.g., fiber optics or satellite)
Latency	Low; minimal delays due to proximity of devices	Very low; ideal for real-time applications within small areas	Moderate; latency increases with distance and traffic volume	High; latency can be significant due to long distances and varied infrastructure
Reliability	Moderate; vulnerable to interference and device limitations	High; reliable within controlled environments like homes or offices	Moderate; reliability depends on the infrastructure and maintenance	Variable; subject to outages due to weather, infrastructure issues, or traffic congestion
Security	High; typically private and limited to personal devices	High; secure within the perimeter but vulnerable to external attacks if not properly configured	Moderate; requires robust security measures due to broader coverage	Low to Moderate; security risks are higher due to global exposure and reliance on public networks
Performance	Suitable for basic tasks like syncing devices or transferring files	Excellent for resource sharing and real-time applications in small areas	Good for city-wide connectivity but may face congestion issues during peak usage	Variable; performance depends on bandwidth availability and infrastructure quality
Applicability	Ideal for personal use, small offices, or residences with limited devices	Best suited for homes, offices, schools, and labs requiring local connectivity	Used by municipalities, universities, or organizations requiring city-wide connectivity	Essential for global communication across countries and continents (e.g., Internet)

Comparative Table: Wired vs. Wireless Networks

Metric	Wired Network	Wireless Network
Bandwidth/Speed	High; speeds can reach up to 10 Gbps with modern Ethernet cables like Cat6 or Cat713.	Moderate; speeds can reach up to 9.6 Gbps with Wi-Fi 6 but are often inconsistent in real-world scenarios
Latency	Low; ideal for real-time applications like gaming and video conferencing due to direct physical connections.	High; prone to delays caused by interference, distance from the router, and network congestion
Reliability	Very high; less prone to interference or signal degradation due to physical cabling.	Moderate; susceptible to environmental factors like walls, electronic devices, and user density.
Security	High; harder to intercept as data travels through physical cables	Lower; more vulnerable to hacking and interception due to open-air transmission
Performance	Excellent; provides stable and consistent connectivity for high-demand applications like streaming and large file transfers	Variable; performance fluctuates depending on interference, proximity, and the number of connected devices
Applicability	Best suited for environments requiring high-speed, secure, and stable connections (e.g., offices, data centers)	Ideal for mobile devices and environments requiring flexibility and ease of installation (e.g., homes, public spaces).

- **Wired networks** are superior in terms of speed, reliability, and security but lack flexibility and mobility. They are best for static setups requiring high performance.
- **Wireless networks** offer greater mobility and ease of installation but are more prone to interference and security vulnerabilities. They are ideal for flexible or dynamic environments.

Application Domains: Suitable Network Types for Industry, Home, and School Environments

The choice between wired and wireless networks varies depending on the unique demands of different environments such as industrial facilities, residential homes, and educational institutions. Each setting has distinct priorities regarding reliability, flexibility, security, and cost-effectiveness.

1. Industrial Settings

- **Recommended Network Type: Wired Networks**
- **Explanation:** Industrial environments typically require highly dependable, fast, and secure network connections to support critical operations like automation, monitoring, and data processing. Wired networks are preferred because they offer consistent performance with minimal interference, which is essential in often harsh and electrically noisy industrial conditions (Fierce Electronics, 2018; Meter.com, 2025).
 - **Benefits:**
 - Stable and reliable connectivity.
 - Enhanced security for sensitive industrial data.
 - Low latency suitable for real-time control systems.
 - **Limitations:**
 - Installation can be costly and less adaptable to changes.

2. Residential Homes

- **Recommended Network Type: Wireless Networks**
- **Explanation:** Homes benefit from the convenience and flexibility of wireless networks, which allow multiple devices such as smartphones, laptops, and smart home gadgets to connect without the need for extensive wiring. Wireless setups are easier to install and support mobility throughout the living space (Meter.com, 2025).
 - **Benefits:**
 - Simple and quick installation.
 - Supports device mobility within the home.
 - Easily expandable to accommodate new devices.

➤ **Limitations:**

- Signal strength may weaken in larger homes or through thick walls.

3. Educational Institutions

- **Recommended Network Type: Hybrid Networks (Combination of Wired and Wireless)**
- **Explanation:** Schools and universities often require a mix of wired and wireless networks to meet diverse needs. Wired connections provide reliable, high-speed access for administrative offices and computer labs, while wireless networks offer flexibility and mobility for students and staff using portable devices in classrooms and common areas (Network Encyclopedia, 2025; PDF Supply Blog, 2021).

❖ **Benefits:**

- Wired networks ensure stable connections for critical infrastructure.
- Wireless networks enable mobility and ease of access across campus.

❖ **Limitations:**

- Managing and maintaining both network types can increase complexity and cost.

Summary Table

Environment	Recommended Network Type	Rationale
Industry	Wired	Provides dependable, secure, and low-latency connections essential for critical industrial tasks.
Home	Wireless	Offers flexibility, ease of setup, and supports multiple mobile devices throughout the home.
School	Hybrid (Wired + Wireless)	Combines the reliability of wired networks with the mobility of wireless access for users.

The choice between wired and wireless networks varies depending on the unique demands of different environments such as industrial facilities, residential homes, and educational institutions. Each setting has distinct priorities regarding reliability, flexibility, security, and cost-effectiveness.

1. Industrial Settings

- **Recommended Network Type: Wired Networks**
- **Explanation:** Industrial environments typically require highly dependable, fast, and secure network connections to support critical operations like automation, monitoring, and data processing. Wired networks are preferred because they offer consistent performance with minimal interference, which is essential in often harsh and electrically noisy industrial conditions (Fierce Electronics, 2018; Meter.com, 2025).

❖ Benefits:

- Stable and reliable connectivity.
- Enhanced security for sensitive industrial data.
- Low latency suitable for real-time control systems.

❖ Limitations:

- Installation can be costly and less adaptable to changes.

2. Residential Homes**• Recommended Network Type: Wireless Networks**

- **Explanation:** Homes benefit from the convenience and flexibility of wireless networks, which allow multiple devices such as smartphones, laptops, and smart home gadgets to connect without the need for extensive wiring. Wireless setups are easier to install and support mobility throughout the living space (Meter.com, 2025).

➤ Benefits:

- Simple and quick installation.
- Supports device mobility within the home.
- Easily expandable to accommodate new devices.

➤ Limitations:

- Signal strength may weaken in larger homes or through thick walls.

3. Educational Institutions

- Recommended Network Type: Hybrid Networks (Combination of Wired and Wireless)
- **Explanation:** Schools and universities often require a mix of wired and wireless networks to meet diverse needs. Wired connections provide reliable, high-speed access for administrative offices and computer labs, while wireless networks offer flexibility and mobility for students and staff using portable devices in classrooms and common areas (Network Encyclopedia, 2025; PDF Supply Blog, 2021).

❖ Benefits:

- Wired networks ensure stable connections for critical infrastructure.
- Wireless networks enable mobility and ease of access across campus.

❖ Limitations:

- Managing and maintaining both network types can increase complexity and cost.

Summary Table

Environment	Recommended Network Type	Rationale
Industry	Wired	Provides dependable, secure, and low-latency connections essential for critical industrial tasks.
Home	Wireless	Offers flexibility, ease of setup, and supports multiple mobile devices throughout the home.
School	Hybrid (Wired + Wireless)	Combines the reliability of wired networks with the mobility of wireless access for users.

Selecting the appropriate network type depends on the specific requirements of each environment. Industrial settings prioritize the stability and security of wired networks, homes favor the convenience and flexibility of wireless connections, and educational institutions benefit from a hybrid approach that balances reliability with mobility.

Discussion:

Trade-offs and Decision-Making: Wired vs. Wireless Networks

1. Wired Networks:

- **Advantages:**
 - **Speed and Reliability:** Wired networks provide faster speeds and stable connections, making them ideal for applications requiring consistent performance, such as video conferencing, gaming, or large file transfers
 - **Security:** Physical connections reduce the risk of unauthorized access, making wired networks more secure for sensitive operations like banking or industrial systems
 - **Low Latency:** Wired connections have minimal delays, essential for real-time data processing
- **Disadvantages:**
 - **Limited Mobility:** Devices must remain physically connected, reducing flexibility
 - **Installation Complexity:** Setting up wired networks is labor-intensive and costly, especially in large spaces
- **Best Use Cases:**
 - Critical environments like data centers, financial institutions, and industrial facilities where reliability and security are paramount.

2. Wireless Networks:

- **Advantages:**
 - **Flexibility and Mobility:** Wireless networks allow users to move freely within coverage areas, making them ideal for dynamic environments like homes or offices

- Ease of Installation: Wireless setups are quicker and less invasive compared to running physical cables
- Scalability: Adding new devices is simple without the need for additional wiring.
- **Disadvantages:**
 - Interference and Latency: Wireless signals are prone to interference from walls, devices, or other networks, leading to slower speeds and higher latency.
 - Security Concerns: Wireless networks are more vulnerable to hacking if encryption is weak.
- **Best Use Cases:**
 - Homes, retail spaces, and educational institutions where mobility and ease of use are prioritized.
- Wired connections can handle critical operations requiring high speed and reliability (e.g., servers or desktop computers in offices).
- Wireless networks can support mobile devices like laptops, tablets, or smartphones for flexibility in shared spaces (e.g., classrooms or meeting rooms).

Hybrid systems are particularly effective in:

- Schools: Wired connections ensure stable internet for computer labs, while wireless facilitates mobility for students and teachers.
- Businesses: Offices often use wired setups for critical tasks (e.g., VoIP systems) alongside wireless access points for employee mobility.
- Homes: A hybrid system can provide wired connections for gaming consoles or streaming devices while maintaining Wi-Fi coverage for mobile gadgets.

Emerging Trends in Networking

1. Wi-Fi 7 (802.11be):

- ❖ Expected to offer speeds up to 46 Gbps with improved latency and reliability. It aims to handle high-density environments like smart homes or crowded offices more effectively than its predecessor Wi-Fi.

2. Low-Latency 5G Networks:

- ❖ With ultra-low latency (<1 ms) and high speeds, 5G is transforming industries like healthcare (remote surgeries) and autonomous vehicles by enabling real-time communication.

3. Optical Wireless Communication (OWC):

- ❖ Technologies like Li-Fi use light waves instead of radio waves for data transmission. They promise ultra-fast speeds with enhanced security but require line-of-sight connectivity

4. Edge Computing Integration:

- ❖ Combining edge computing with networking technologies allows faster data processing closer to the source, reducing latency in applications like IoT devices or smart factories.

The decision between wired and wireless networks depends on specific needs such as speed, reliability, security, and mobility. While wired networks excel in stability and performance-critical environments, wireless networks offer unmatched flexibility and ease of use. A hybrid system often provides the best of both worlds by balancing reliability with mobility. Emerging technologies like Wi-Fi 7, 5G, and optical wireless will further shape the future of networking by addressing current limitations while enhancing speed, security, and scalability.

Conclusion

This paper has provided an in-depth comparison of wired and wireless networks, focusing on their suitability across various settings such as industrial environments, homes, and educational institutions. Wired networks are known for their high speed, dependable performance, and strong security, making them well-suited for critical applications that demand consistent connectivity. On the other hand, wireless networks offer greater flexibility, simpler installation, and scalability, which are essential for environments that require mobility and adaptability.

By evaluating key factors like bandwidth, latency, reliability, and practical use cases, it becomes clear that no single network type fits all scenarios. The best choice depends on the unique needs of each environment. With the increasing use of digital platforms, remote education, and smart devices, selecting the right network infrastructure—or combining both wired and wireless technologies—has become more important than ever. Hybrid networks, which leverage the benefits of both types, are especially advantageous in places like schools where both stable connections and mobility are necessary.

Recommendations

Industrial sectors should focus on wired networks to ensure secure and stable real-time communication.

Organizations should proactively invest in next-generation technologies like Wi-Fi 7, 5G, and Li-Fi. These innovations offer significant enhancements in speed, reduced latency, and greater scalability, supporting the demands of modern digital environments.

Plan for Future Growth and Maintainability
Network infrastructure should be designed with future expansion in mind. This includes ensuring the ability to support an increasing number of devices and higher bandwidth demands, as well as simplifying maintenance especially in hybrid network environments.

References

Berners-Lee, T., & Fischetti, M. (2019). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. Harper.

Fortinet. (2025). *What Is a Wireless Network? Types of Wireless Networks*. Retrieved from Fortinet.com.

Goldsmith, A. (2021). *Wireless Communications* (2nd ed.). Cambridge University Press.

- Kurose, J. F., & Ross, K. W. (2020). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Ruckus Networks. (2025). *Wireless Network Technology: A Comprehensive Overview*.
- Stallings, W. (2017). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley.
- TutorialsPoint. (2021). *What Are Wireless Networks?* Retrieved from TutorialsPoint.com.
- TutorialsPoint. (2025). *Wireless Networks Overview*. Retrieved from TutorialsPoint.com.
- Kurose, J. F., & Ross, K. W. (2020). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Stallings, W. (2017). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley.
- Tanenbaum, A. S., & Wetherall, D. J. (2014). *Computer Networks* (5th ed.). Pearson.