



Wireless Local Area Networks: Architecture, Security, and the Transformation of Enterprise Connectivity

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract – Wireless Local Area Networks (WLANs) have grown from a convenience feature to become the main medium of access for enterprise, residential and industrial computing. This article will delve into the basics of the technology, its working principles, standards, and its significance in the current digital landscape. The talk will discuss the evolution of radio-based local networking from wired dependence, the development of the IEEE 802.11 family of standards and the creation of the Wi-Fi ecosystem, and the recent arrival of new frequency bands at 6 GHz, which will increase capacity in dense environments. Focus is placed on the layers of architecture used to support large deployments, including access points, wireless controllers and segmentation techniques like VLANs. The paper also covers the security stance necessary to secure wireless traffic, such as the latest in encryption standards and policy-based access control as well as the operational challenges that remain and impact performance and reliability. The analysis of 2026 trends is dedicated to the fast adoption of Wi-Fi 7, the new Wi-Fi 8 ultra-reliability standard and the use of artificial intelligence to manage wireless platforms. The article ends with a discussion on the future prospects of WLANs in supporting developments in robotics, extended reality and autonomous operations and provides some practical considerations for organisations looking towards a long-term wireless strategy.

Keywords: WLAN, Wireless LAN, Wi-Fi 7, WLAN security, Wi-Fi 8, Wireless networking, Enterprise WLAN, WLAN architecture.

1. INTRODUCTION

The unobtrusive change from copper wire to radio waves in local networking is among the most significant changes in information technology over the past 30 years. A simple project to unplug office workstations from Ethernet has turned into the most popular way that people and machines connect to digital services. Wireless local area networks (WLANs) handle most of the traffic within homes, campuses, hospitals, factories and transportation facilities today. Knowing how these networks work, where they're going and how to responsibly deploy them has become a critical part of the digital infrastructure curriculum. This article is an organized analysis of the WLAN technology. It starts with clarity of definitions, progresses to architectural elements, and concludes with a focus on the technological changes that are occurring until 2026 and beyond. The aim is to offer a comprehensive reference that is practical, reflects the latest in engineering practice and is aware of the strategic implications for organisations looking towards the next 10 years of connected operations.

2. WHAT IS A WLAN

A wireless local area network (WLAN) is a type of LAN that transmits data between endpoints in a specific geographic area via radio frequency (RF). The size of the footprint can range from a single apartment to

an industrial campus with a surface area of several square kilometers. The common characteristic of each is that there is no permanent connection between the endpoint and the first network device that provides a service to the endpoint.

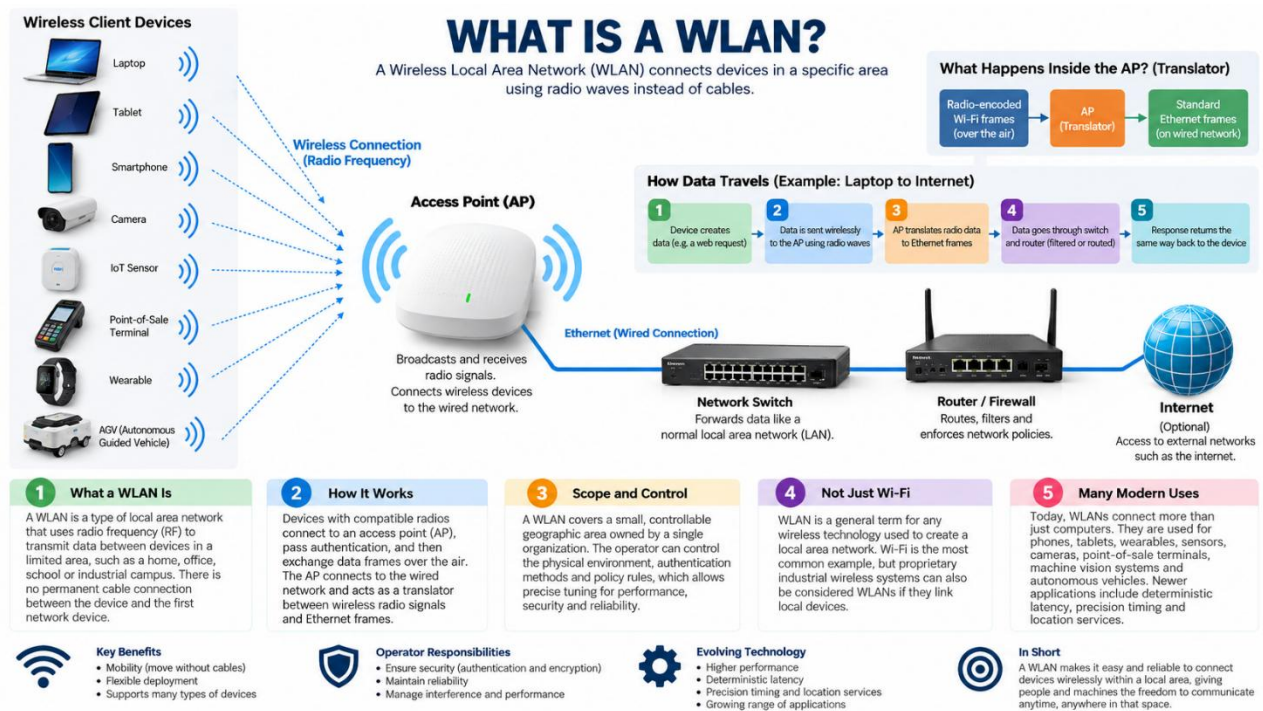


Fig -1: What is WLAN

The technical premise is very simple. An access point is a device that is connected to the wired backbone that broadcasts and receives radio signals in an area. Client devices with compatible radios join to the AP, pass the authentication and then start to exchange data frames over the air. The access point is a translator between radio-encoded traffic and Ethernet frames which are transmitted over the wired part of the network. When traffic crosses to the wired side, it's treated as any other local area network communication and can be routed, filtered or forwarded as usual.

There are a number of differences that should be noted when discussing WLANs professionally. The term is used to describe any wireless technology that can be used to establish a LAN (local area network), it is not a technical specification. The most common form of use is Wi-Fi, but this isn't the only one. Certain proprietary industrial wireless systems also can be considered WLANs if they are used to link local nodes. The geographical and administrative range of a WLAN is the scope. Unlike wide area networks (WANs), which span public or carrier networks, it is small enough to be controlled by a single ownership domain. This locality implies that the WLAN operators are able to control the physical environment, the authentication framework and the policy enforcement rules. That's a good thing as it means it can be tuned precisely, but it's also a responsibility as it means that the owner has to take care of security and reliability.

The development of WLANs is a trend in the development of computing. While the early networks were used to connect desktop computers at a fixed location, today's WLANs are used to connect mobile phones, tablets, laptops, wearables, sensors, cameras, point-of-sale terminals, machine vision systems, and automated guided vehicles. WLAN engineering is now being applied in new areas such as deterministic

latency, precision timing, and location services, which were all secondary considerations just a decade ago, as WLANs have diversified their applications.

3. WLAN EXPLAINED IN TECHNICAL TERMS

A closer examination of the WLAN concept shows that it is a layered system and is not one technology. In practice a WLAN is a set of coordinated layers that provide wireless connectivity. Radio transceivers modulate binary data into electromagnetic waves at the physical layer, by using techniques like quadrature amplitude modulation and orthogonal frequency division multiple access. The medium access control sublayer is responsible for the sharing and collision avoidance of the medium among multiple devices at the data link layer, for example, carrier sensing and request to send.

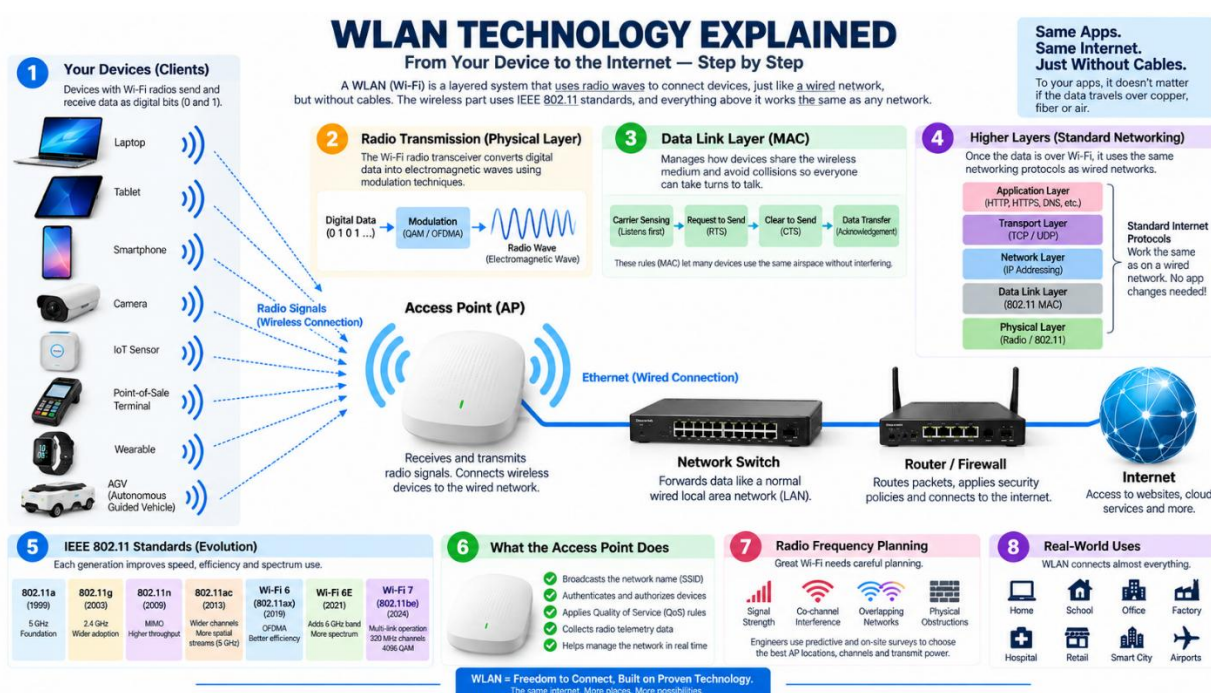


Fig -2: WLAN Technology Explained

On top of these basic layers, the WLAN can use the entire suite of standard networking protocols. Internet Protocol addressing and transport layer protocols (TCP and UDP) along with application protocols work as they would on any wired network. This is a design decision and not a coincidence. Retaining the compatibility of the wireless part with the higher layers of the networking stack meant that applications wouldn't have to be re-written to work wirelessly. Whether a packet is traveling over copper, fiber or air is irrelevant to, and doesn't need to be known by, a browser, a database client, or a video conferencing tool.

The most common implementation of WLAN is controlled by the IEEE 802.11 family of standards. Over the past several generations the family has undergone various changes and improvements in throughput, efficiency, and spectral use. Previous amendments, such as 802.11a and 802.11g, laid the groundwork. The 802.11n standard was the first standard to introduce multiple input multiple output antenna technology. The 802.11ac standard brings with it wider channels and more spatial streams on the 5 GHz band. Wi-Fi 6 (802.11ax) introduced orthogonal frequency division multiple access, and extended the operation to the 6

GHz band, which is now called Wi-Fi 6E. The latest ratified amendment, 802.11be (Wi-Fi 7), added multi-link operation, 320 MHz channels and 4096 quadrature amplitude modulation.

Access points serve multiple functions as hardware anchors of a Wi-Fi WLAN. They broadcast service set identifiers which are then detected by clients while scanning. They validate devices that want to associate with the local or remote credential store. They implement Quality of Service policies that give preferential treatment to traffic like voice. They also gather telemetry data on radio conditions, which is used to feed into network management systems that tune in the environment in real-time. Careful radio frequency planning is also essential to a properly designed WLAN. Performance is affected by signal strength, co-channel interference, interference from overlapping networks and physical obstructions. Predictive and empirical site surveys are often undertaken by the engineers to decide on the location of access points and the power at which they are to be transmitting. Even the most sophisticated wireless equipment will not perform to its fullest potential if this foundation is not present.

4. IS WLAN THE SAME AS WI-FI

Many people are confused and equate WLAN with Wi-Fi, both in technical discussions and everyday life. The two terms are similar, but not synonymous. A WLAN is a general term that refers to any type of local network that uses wireless transmission. Wi-Fi is a particular family of standards, certified by Wi-Fi Alliance, that are based on IEEE 802.11 standards. While all Wi-Fi networks are WLANs, not all WLANs are Wi-Fi networks.

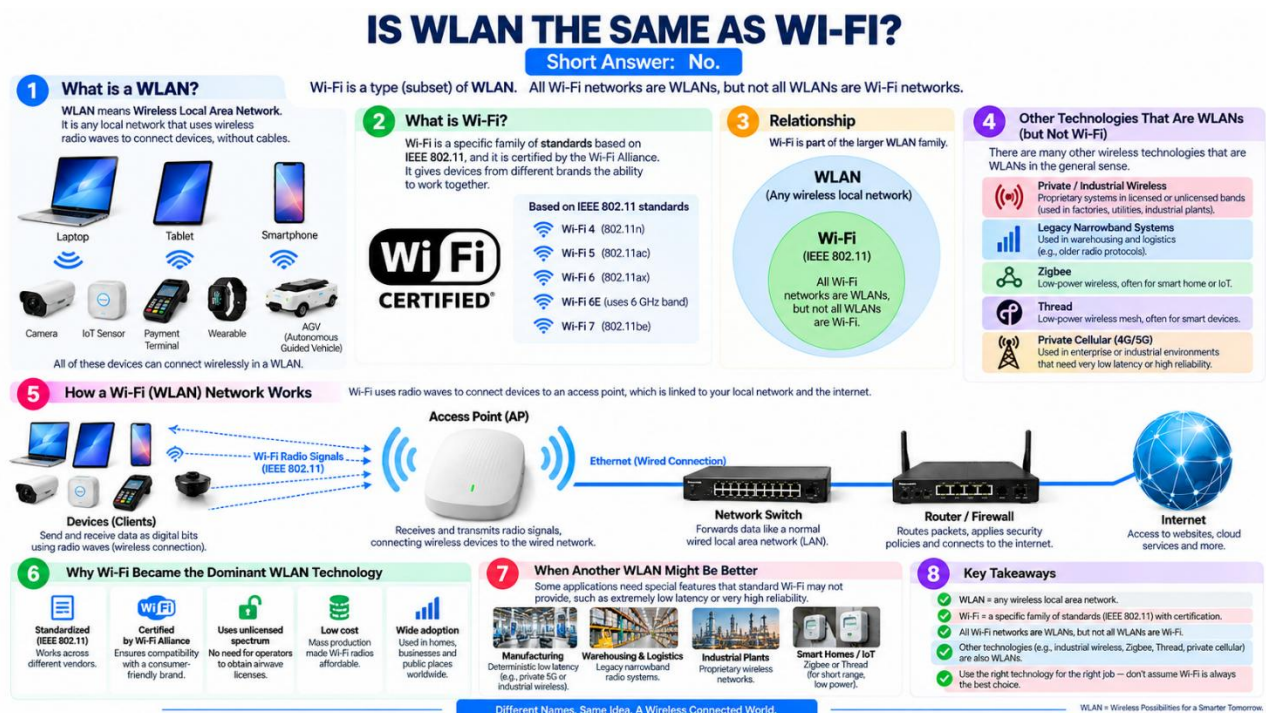


Fig -3: Is WLAN the Same as WI-FI

There are a number of other technologies which can be considered WLANs in the general sense. Certain industrial plants use proprietary wireless systems in licensed or unlicensed bands that are used to link sensors, controllers and actuators in a local area. There are still some legacy systems in use in warehousing



and logistics that are based on narrowband radio protocols. Low-power personal area networks like Zigbee or Thread, when used to link a limited number of nodes, also live in a similar functional space, but are usually considered personal networks, rather than local networks because of their limited range.

Wi-Fi is the dominant technology in WLANs for a number of reasons. Equipment from different vendors was standardized under IEEE, reducing the risk of deployment, and thus driving adoption. When the Wi-Fi Alliance certified it, it was given a consumer-friendly brand that indicated compatibility. The regulators in various jurisdictions decided to make unlicensed spectrum available for Wi-Fi, thus removing the need for operators to obtain airwave licenses. Lastly, the economics of mass production reduced the cost of Wi-Fi radios to the point where they could be routinely used in nearly all consumer and professional devices.

Although it's easy to see how the two terms can be mixed up, it's important to get it right in professional environments. If procurement teams say they need a WLAN, they are typically referring to Wi-Fi, but that's important when considering other solutions for specific applications. A manufacturing environment that requires deterministic latency at the millisecond level may determine that standard Wi-Fi isn't the best solution and may opt for a private cellular network or an industrial wireless protocol. These are all WLANs in the general sense, but not Wi-Fi. Definitions also are important for tracking standards. Documents which discuss the performance of WLANs in general may use a different test methodology than those which specifically test Wi-Fi equipment. Analysts, administrators and architects benefit from a clear hierarchy as it helps to avoid misunderstandings and to ensure that the technology chosen is the one that is truly needed, not just assumed because of the brand.

5. WHY WLAN THE FORCES DRIVING ADOPTION

Over the years, the rationale behind organizations investment in wireless local networking has changed significantly. Convenience and mobility were the motivators for adoption in the first wave. Staff requested to bring laptops to conference rooms. Students were interested in working in libraries but couldn't locate a free Ethernet jack. Those motivations remain, but are now accompanied by much more significant ones. One of the most important trends that is driving WLAN demand is the proliferation of the Internet of Things (IoT). The number of connected devices has been estimated by industry to be tens of billions, and the amount of data generated by sensors to be tens of zettabytes per year. All of these endpoints need to be reliable, secure and, in many cases, low power. WLANs have emerged as the standard medium for the connection of these devices, since they offer a wide range of availability, low individual device cost and can be managed by the existing network management system.

Diversity of application is a second driver. Today, latency-sensitive applications like video conferencing, cloud gaming, real-time collaboration and immersive media make up a significant portion of enterprise and consumer bandwidth. In the latest reporting periods, market observations have put the growth rate of latency-sensitive video applications at almost forty-five percent per year. Every new type of application has its own requirements for the wireless infrastructure. In order to maintain voice calls, jitter control is required. Low motion to photon latency is required for VR. Deterministic timing is needed for industrial control. A WLAN, which is only capable of carrying general purpose web traffic will not suffice these requirements.

There is a third force user expectations. There is now a low tolerance for network performance problems. Whether it is employees, customers or guests, end users expect the network to be like a utility, on at all times, available to everyone and invisible when operating. The reputational price point of a poor wireless

experience has increased to the point where executives are getting direct feedback from top stakeholders regarding the quality of Wi-Fi in the office, retail store or event venue. This feedback loop has resulted in the performance of WLANs being a board-level issue in some organizations.



Fig -4: Why WLAN

The needs of businesses have also grown when it comes to mobility and roaming. Employees travel from building to building, campus to campus and from client site to client site during their workday. Telemetry systems are installed in vehicles and these systems are used to move vehicles around warehouses and ports. Cellular offload – the ability to hand off from carrier networks to local Wi-Fi is no longer a luxury, it is a necessity. These capabilities require well-engineered WLANs that can support handoffs between access points without interrupting on going sessions. Last, the role of the local network has changed with cloud computing. Wired data center was the critical infrastructure when applications were on local servers. In a cloud first world the WLAN is frequently the last infrastructure an organization has direct control over between the user and the application. That change has made wireless a strategic asset, rather than a side-line service.

6. THE ROLE OF WIRELESS CONTROLLERS IN WLAN ARCHITECTURE

Wireless controllers are a key component of enterprise WLANs. They are used to synchronize the actions of a set of access points to act as a single entity and not as separate entities. For small deployments, where there are just a few access points, controller functions can be integrated into the access points, or provided via a cloud management platform. In larger deployments, there is an orchestration layer that maintains stability at scale, either as a separate controller or as virtual controllers. There are a number of functions that the controller is responsible for. Among the most important is radio resource management. In a large campus, multiple access points contend for limited spectrum, without interfering with each other. The

controller collects data from each AP regarding its radio environment such as the use of channels, noise levels and adjacent signals and then makes configuration changes. The changes include changing channels, changing transmit power, or steering clients to less congested APs. If done correctly, radio resource management will double the effective capacity of a WLAN.

THE ROLE OF WIRELESS CONTROLLERS IN WLAN ARCHITECTURE

One Brain. Many Access Points. A Better, Smarter, Safer WLAN.

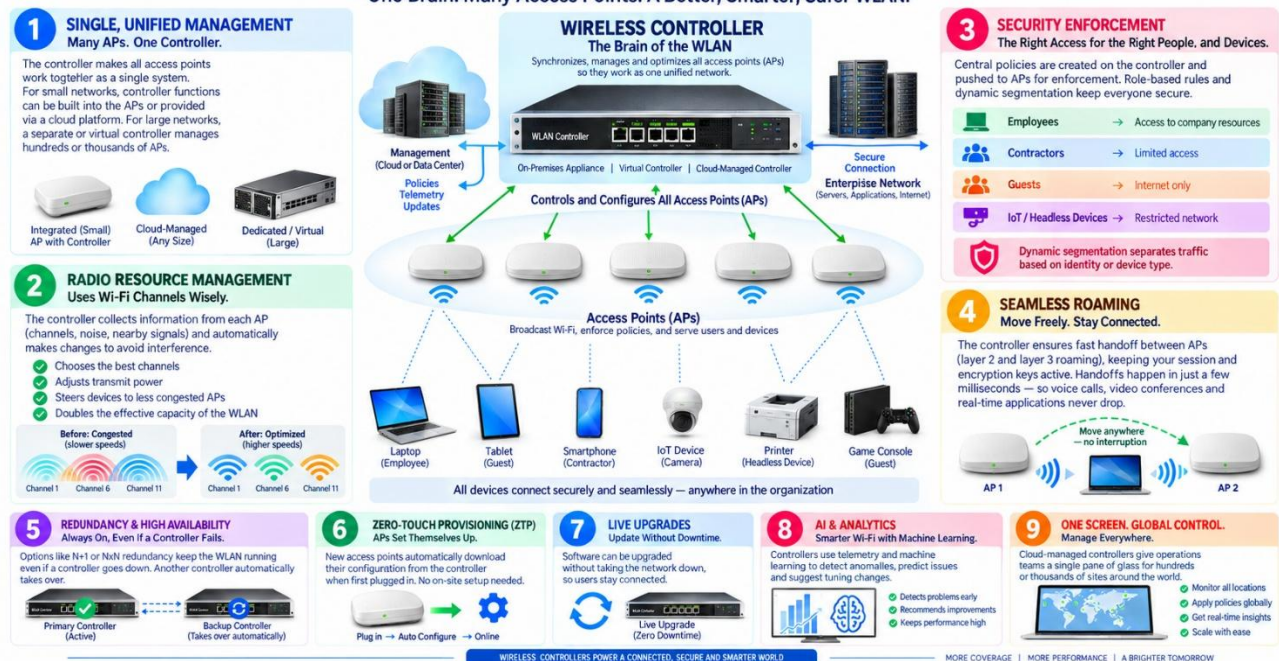


Fig -5: The Role of Wireless Controllers In WLAN Architecture

One of the fundamental controller roles is security enforcement. Central policies are created to determine access to specific resources by user and or device and are pushed to the edge for enforcement at the access points. Role based rules enable the administrators to distinguish between the employees, contractors, guests and headless devices and restrict them accordingly. Dynamic segmentation traffic is directed into separate logical pathways according to identity or device type has become a standard feature. Controllers are also helpful in a third area: roaming. As a device moves from the reach of one access point to another, the handoff between the two needs to be quick enough that any applications using the device are not aware of the handoff. Modern controllers will take care of layer two and layer three roaming between virtual LANs, maintaining the state of the session and encryption keys, making the handoff just a few milliseconds. This is a must have for voice calls, video conferences and real-time applications in industry.

Redundancy is also an issue for controllers. In enterprise environments, the failure of one controller cannot impact the services. Redundancy options like N+1 and NxN redundancy provide for another controller to assume control in the event of the primary controller failure. These features, coupled with the zero-touch provisioning (ZTP) that automatically provisions new access points on first boot, decrease the burden on on-site technical staff. The newer generation of controllers, many of which are provided as cloud managed services, has capabilities that are not possible with the previous appliance-based designs. Live Upgrades Software can be upgraded without taking the network down. Machine learning systems that detect

anomalies and suggest tuning changes are fed with telemetry streaming. With hundreds or thousands of locations under one management, operations teams have one pane of operations for their globally distributed infrastructure.

7. WLAN VERSUS VLAN CLARIFYING THE DISTINCTION

One of the most frequently used terminological confusions that pertain to network discussion is the difference between WLAN and VLAN. While there is no relationship in function, there is enough similarity in letters that casual readers may mix up the two concepts. It's important for anyone designing or managing a network to know what each is.

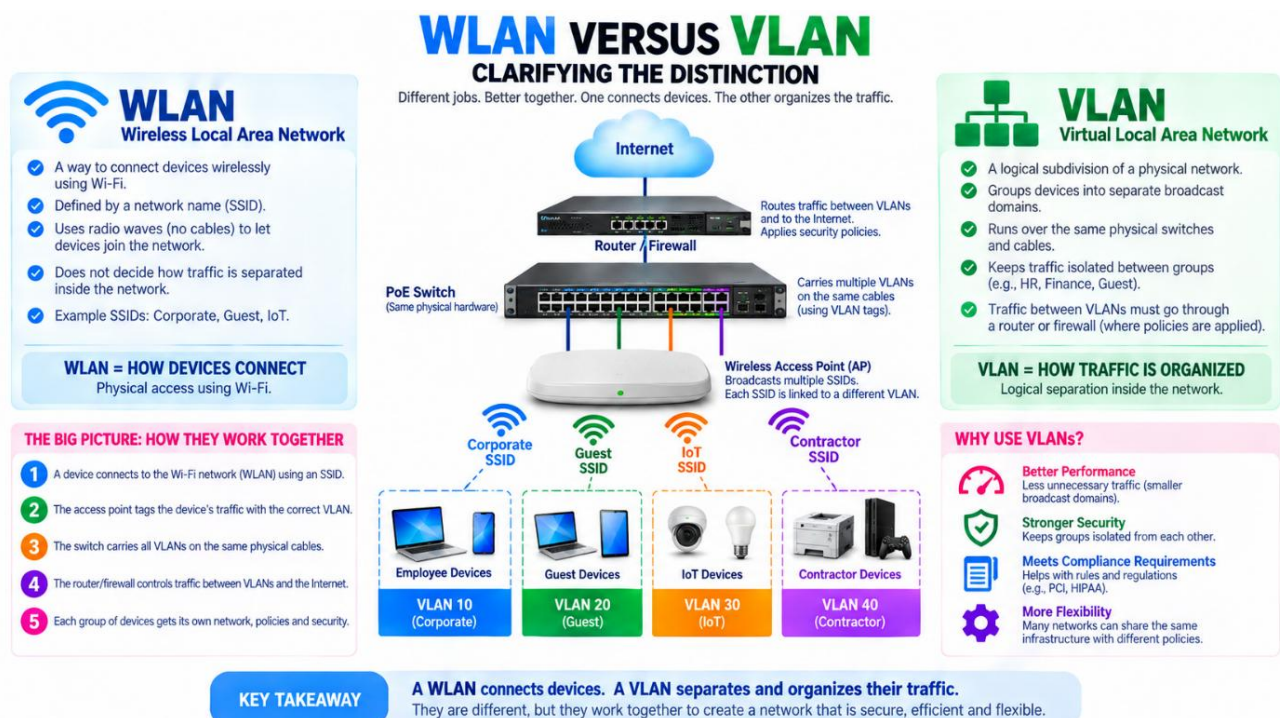


Fig -6: WLAN Versus VLAN

VLAN is a virtual local area network (VLAN) that is a logical subdivision of a physical network. It provides the ability to transport traffic for a number of distinct broadcast domains over a single physical infrastructure. An organization might choose to create separate network segments for the human resources department, the finance department and the guest wireless users, even if they have one physical switch fabric, by assigning each of these groups to its own VLAN. The traffic in a VLAN acts as if it were on a separate physical network, and traffic between VLANs must go through a router or firewall, which can apply policy.

Performance and security are the reasons to segment with VLANs. Performance wise, broadcasts and other overhead traffic are limited to a smaller number of devices, decreasing unnecessary traffic. Security wise, isolation between segments prevents a compromised device from communicating with other devices that it shouldn't be able to communicate with. Network segmentation is either explicitly or implicitly mandated by many compliance regimes and VLANs are the typical way to perform this segmentation. In contrast, a WLAN is a way of physically connecting and not a logical partition. It is a definition of the devices

attachment to the network, not of the organization of the traffic once it reaches the network. This is commonly a problem when multiple service set identifiers are used on the same wireless infrastructure and each service set identifier is assigned to a different VLAN. In this design, users connecting to the corporate SSID will be on the corporate VLAN, users connecting to the guest SSID will be on the guest VLAN. The access point is used by both, but traffic is tagged and segregated according to the wireless network that the user joined.

This combination design is very popular and illustrates how WLANs and VLANs are complementary and not competing. Many logical networks can share the same physical wireless infrastructure, each having its own policies, security posture and bandwidth allowances. This flexibility is one factor that makes it possible for modern organizations to support employees, contractors, guests and Internet of Things devices all from the same deployed infrastructure without any compromise to security or performance. It's easy to mix up the two, and this can result in serious design mistakes. A plan that assumes WLAN and VLAN are interchangeable could result in a lack of isolation of sensitive traffic or in an inefficient use of radio resources. Therefore, it is important to distinguish between the two terms in the documentation and architectural diagrams.

8. HOW A WLAN WORKS

To get a true sense of the operation of a WLAN, a frame of data must be tracked from the time it leaves a client device until it reaches its destination. This includes radio propagation, protocol handshakes, and backbone forwarding, all in a matter of fractions of a second.

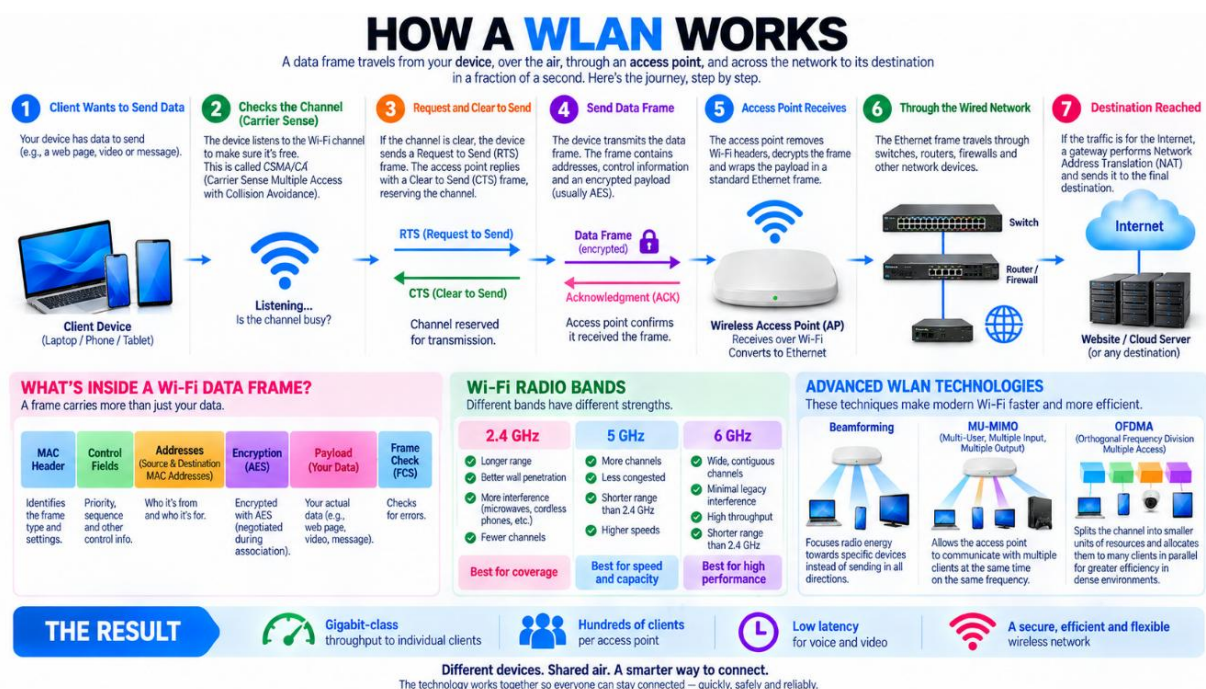


Fig -7: How A WLAN Works

The first step in the process is when a client device wants to send data. The device checks the radio channel before transmitting to make sure that no other device is transmitting on that channel. This is called carrier



sense multiple access with collision avoidance, and is at the heart of WiFi's approach to sharing the spectrum. If the channel is not busy, the device can send a request to send frame to the access point. The access point returns a clear to send frame, thus reserving the channel for the pending transmission. The client then transmits its data frame and the access point confirms that it has received the frame. More than just the payload is in the data frame. It includes addressing information such as the sender's and receiver's media access control addresses, control fields to specify the frame type and priority, and encryption fields to secure the payload. In today's modern WLANs, the payload is very rarely sent in the clear, but is instead encrypted with advanced encryption standard (AES) ciphers negotiated during the association phase.

The frame is received by the access point, which removes the wireless specific headers and wraps the payload in a standard Ethernet frame. This Ethernet frame is then sent out over the wired backbone, which could go through a number of switches, routers, firewalls and other network devices before arriving at its destination. If the frame is for Internet traffic, the frame usually is forwarded to a gateway that will do network address translation and send the packet to its external destination. The propagation properties of the bands used by Wi-Fi are different at 2.4 GHz, 5 GHz, and 6 GHz. The 2.4 GHz band is capable of transmitting farther and penetrating walls more effectively, but has limited channel capacity and a lot of interference from non-Wi-Fi devices like microwave ovens and legacy cordless phones. The 5 GHz band offers greater channels and is typically less congested, but has a shorter range. The 6 GHz band, which opened to Wi-Fi use more recently, has wide contiguous channels, and minimal legacy interference, which makes it perfect for high throughput applications.

More than one antenna is used to improve performance in today's WLANs. Beamforming is a technique where radio energy is directed towards specific clients instead of omnidirectional. Multiple users, multiple inputs, multiple outputs (MU-MIMO) enables the access point to communicate with multiple clients at the same time on the same frequency. OCDMA splits channels into smaller units of resources, and allocates them to various clients in parallel, thus increasing the efficiency in dense environments. All of these techniques work together to enable a well-designed modern WLAN to provide gigabit-class throughput to individual clients, hundreds of concurrent clients per access point, and latency low enough for voice and video applications. There are still physical constraints on radio transmission, but engineering ingenuity has taken them much farther than they appeared to be a few years ago.

9. BENEFITS OF USING A WLAN

Wireless Local Area Network deployment can have a positive impact on operational, financial and strategic levels. The most apparent advantage of mobility is the mobility itself. Users and devices are able to roam in the coverage area without any disconnection. This freedom for office workers means that they can work from any desk, conference room or common area. For warehouse staff, it means scanning inventory from anywhere on the warehouse. It also translates to the ability for medical staff to access patient records at the patient's bedside instead of going back to a workstation. Another major advantage is scalability. There is no need to add any physical infrastructure to add new users to a WLAN, other than making sure coverage is sufficient. By contrast, a wired network requires pulling cable, terminating connections and provisioning switch ports to add users to the network. The ability to quickly onboard a large number of devices can mean the difference between a successful rollout and a stalled project, during times of rapid growth, organizational mergers or temporary events.

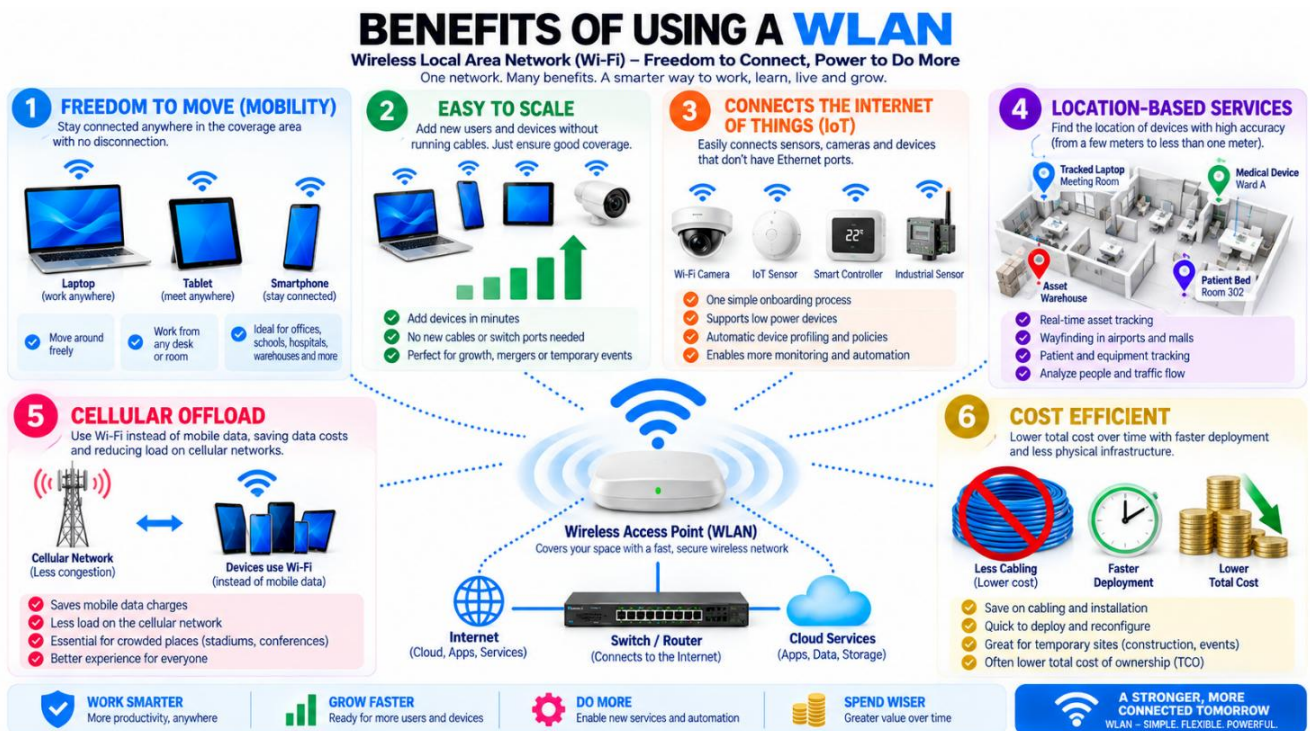


Fig –8: Benefits of Using A WLAN

Connectivity with the Internet of Things is a welcomed feature and is becoming more and more significant. There are numerous sensors, cameras and controllers that do not have Ethernet ports and even if they did, they would be impossible to wire. A WLAN offers a common onboarding process for these types of devices, and may include functionality that is specifically tailored for their use, including low power operation, device profiling and automated policy assignment. This flexibility of sensor positioning not cable positioning opens up a multitude of monitoring and automation opportunities.

One of the advantages of which is not always recognized is location-based services. Modern WLANs are able to identify the location of a connected device with a few meters up to less than one meter of accuracy, depending on the density of access points and the specific features that are available to the WLAN. This ability can be used for asset tracking, in hospitals and warehouses, for wayfinding, in airports and shopping centres, and for analytics of traffic flow in retail environments. Knowing where things and people are, in real time, continues to fuel investment in WLAN infrastructure for the business. Another advantage to mention is that of cellular offload. Mobile devices use WLANs so they do not have to use data allowances on their cellular devices. For end users, this saves data charges. In an enterprise context, it lessens the load on the cellular backbone in areas where a number of devices would otherwise battle for scarce carrier bandwidth. In other locations, like stadiums or conference centers, it is critical to offload cellular traffic to Wi-Fi in order to provide acceptable service.

Although it is difficult to put a number on cost efficiency, it can be considerable. These savings are cumulative over the life of a facility, due to avoided cabling, faster deployment and reconfiguration. On a temporary site like a construction site or event venue, the economics are very much in favor of wireless. In

even the most permanent installations, the TCO of a wireless first approach to client access may often be the better choice, as wired infrastructure is used for backbone connections and fixed equipment.

10. ADVANTAGES OF WLAN OVER TRADITIONAL WIRED LAN

It helps to compare WLAN with its wired predecessor, which will help to clarify the understanding of what WLAN really provides. The most apparent benefit is that there are no longer physical cables connecting the client device to the network. This one change affects the deployment and operation of the network in all aspects.

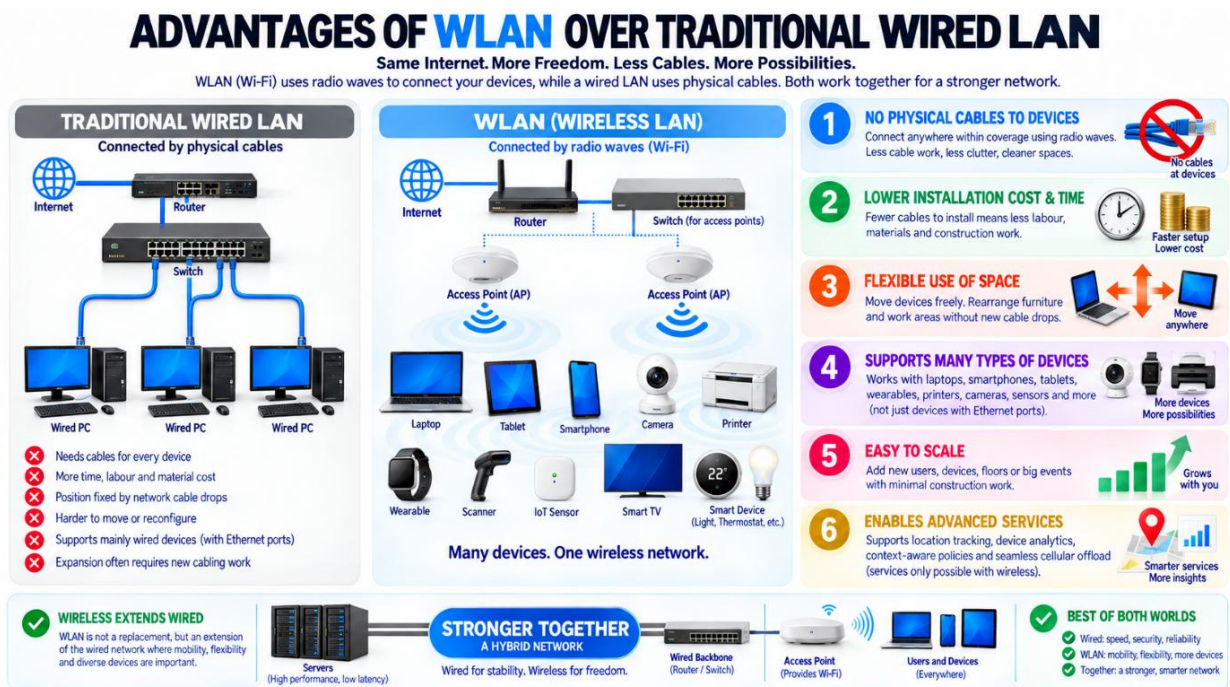


Fig -9: Advantages of WLAN Over Traditional Wired LAN

The lack of cables significantly cuts installation time, labour and material costs in bringing a new facility on-line. With a traditional wired deployment, each workstation must have a cable installed and run from the data closet to the workstation, the cable must be pulled through walls, ceilings and floors, both ends must be terminated and the cable must be tested. While access points still need cabling in a wireless deployment, the number of cables is reduced, and the majority of the work area is free of cables. The savings in construction, particularly in historic structures or temporary structures can be significant. Flexibility in the use of space is another advantage. With wired network, the position of network drops determines the position of workstations. When an office is reconfigured, they either have to settle for a suboptimal office configuration or spend money to add additional drops. A wireless environment does not put such a restriction. Devices can be moved around and furniture, equipment and work areas can be arranged as required to suit the functional needs of the network. This versatility has proven particularly useful since many businesses are trying out hybrid work models, hot-desking and shared work areas.

An added benefit that isn't as obvious is support for different devices. The wired LAN was developed as a network for stationary devices that have Ethernet ports. A WLAN can support smartphones, tablets, laptops,



wearables, scanners, cameras, printers, sensors and dozens of other types of devices, many of which are not wired devices. The range of connection points that can be attached to a WLAN is much greater than can be attached to a wired network. Another advantage is the ability to quickly scale to meet growth demand. Addition of new employees, new floors or big events are handled by the WLAN without any construction work. The physical infrastructure can be added to and configurations can be tweaked, but the basic physical infrastructure does not need to be altered extensively. This agility is the same as that of today's business decision making.

Another plus is the capacity to provide advanced services. Things like location tracking, device analytics, context-aware policy enforcement and seamless cellular offload are hard or impossible to do on a wired-only network. These services require information that can only be gathered from a wireless infrastructure, like radio signal strength from various access points to enable triangulation or roaming patterns of the devices to enable behavior analysis. That isn't to say wired networks are out of the question. Wired paths still have the advantage of latency, security and determinism for backbone connectivity, server interconnection and high reliability industrial control. The modern network is a hybrid network, that is, wired and wireless networks are working together. The benefit of WLAN is not that it is to be used as an alternative to the wired network but that it is an extension of it in every corner of the physical environment where mobility, flexibility and diversity of devices is important.

II. SECURITY MEASURES FOR WLAN

Security is the most important consideration and the fastest changing aspect of WLAN engineering. Wireless signals penetrate the walls of a building, which means they can be accessed from outside the network, making the attack surface larger than wired networks. Any opponent in the radio range is able to try and communicate with the network at least. There's no single solution to combat this reality, and it will take a layered approach. The basis layer is encryption. The current generation of WLANs are based on Wi-Fi Protected Access version 3 (WPA3), which superseded previous mechanisms that were compromised. WPA3 adds simultaneous authentication of equals, a key exchange protocol that is immune to offline dictionary attacks and enhances the enterprise authentication cryptographic suites. The transition from WPA2 to WPA3 has been slow and steady and most new enterprise access points are set to WPA3 or can be set to accept both.

One of the traditional weak points has been guest access, as open networks provided none of the encryption. Wi-Fi Alliance's Enhanced Open is a mode that will give opportunistic wireless encryption, meaning that data in transit will be encrypted even on networks that don't require a password. This feature addresses the missing link in public and semi-public Wi-Fi networks like cafes, lobby areas and visitor areas. A second important level is authentication. Enterprise WLANs are usually used in conjunction with a centralized identity system, using the 802.1X framework. As each user or device submits credentials **username/password, digital certificate, or token**, the access point checks with an authentication server before providing access. This design enables credentials to be revoked centrally when an employee leaves or a device is lost and enables strong forms of authentication, like certificate-based login, which are resistant to phishing.

Policy enforcement goes beyond authentication, and continues with traffic control. Role-based access rules can be used to implement different policies for different groups of users and devices. A finance employee can access the accounting application servers, but a guest device can't see the application

servers. Modern wireless infrastructure incorporates policy enforcement firewalls at the edge, so that unauthorized traffic is denied at the point of entry into the network, instead of being denied later in the network.



Fig -10: Security Measures For WLAN

Dynamic segmentation can be used in addition to role-based access to automatically move traffic from various classes of devices into their own logical networks. If a camera joins the WLAN, it is put into a camera specific segment, where only communication patterns typical for cameras are allowed. The segmentation restricts what damage can be done if the camera is at a later stage compromised and starts acting abnormally. The last security level is monitoring and detection. Rogue access point detection is a process of detecting unauthorized radios that are operating in the organization's airspace. Wireless intrusion prevention systems detect common wireless attack types including evil twin, deauthentication flood, and credential harvesting attempts using known attack patterns. Anomalies that could only be identified by hand at thousands of devices are identified by machine learning tools, which are increasingly being integrated into wireless management platforms. The security posture is completed with operational practices. Firmware needs to be updated on time to patch known vulnerabilities. Access points and controllers need to have their default credentials changed. Site surveys should take into account adversarial perspective, which is where an adversary may be located and what signals they may be able to see. WLAN security only withstands the determined threats when technology and process collaborate.

12. COMMON ISSUES WITH WLAN CONNECTIONS

Although there has been progress in technology, WLAN deployments have been plagued by the same set of issues. Knowing these problems assists administrators in diagnosing complaints as well as creating a more resilient network.

COMMON ISSUES WITH WLAN CONNECTIONS

Understanding these common problems helps build a more reliable, faster and stronger wireless network.
Different factors can affect Wi-Fi. Here are the main issues, what causes them, and how to fix or reduce them.



Fig -11: Common Issues With WLAN Connections

One of the most frequent complaints is about poor performance while roaming. Ideally, if a device leaves the coverage area of one access point and enters another, it should switch seamlessly, but in reality, devices may not move on to a new access point until they are no longer in the range of the original access point. This is known as sticky client syndrome and results in loss of throughput and dropped sessions. There are two aspects to mitigation: access point configuration e.g., prompt early disassociation due to signal strength and client-side behavior which is different for each client vendor. Another constant problem is spotty connectivity in high-density environments. Devices are often used in large numbers in small spaces such as conference rooms, stadiums, lecture theatres and open plan offices. Despite the current spectrum sharing methods, the available capacity might not be sufficient during peak time. This can manifest itself as slow page loads, failed authentication attempts and dropped video calls. These problems need to be solved with careful design of the radio frequencies, including access point placement, antenna selection and channel planning, and capacity-oriented features of access points.

Coverage gaps in buildings are commonly reported as the original design is based on assumptions that no longer apply. Previously a storage room, it's now a meeting room. Signals might have been obstructed by the rearrangement of furniture. Additional walls or partitions may have been constructed. These holes can be identified with periodic site surveys and automated coverage analysis, before users complain. The limited connectivity options for Internet of Things (IoT) devices causes other issues. Many IoT devices are only compatible with older Wi-Fi standards, or don't have enterprise authentication features or require particular configurations. Backward compatible SSIDs are often required to support these devices, which are less efficient in using spectrum, or a separate infrastructure to handle IoT traffic.

For video and streaming services, high latency can impact users experience even if raw bandwidth is sufficient. Latency can be added up from many places, such as retransmissions at the radio level, forwarding paths in the controller and congestion in the wired backbone. To troubleshoot latency, end-to-end visibility is needed from the wireless, wired and upstream. Spectrum management techniques are still



not working well interference from other networks and non-Wi-Fi devices is still causing issues. Noise can be added to Wi-Fi bands from microwave ovens, Bluetooth devices, wireless cameras and even some lighting systems. Multi-tenant buildings can have access points from other tenants that are the same frequency, which decreases the effective capacity of all access points.

Client device issues can be caused by out-of-date firmware and drivers. A client running an outdated driver version might not be able to take advantage of new features, might not be able to correctly interpret the standards compliant signaling, or might be unstable. These issues are reduced if users are encouraged to keep their devices up to date and compatibility testing is done on common client platforms. Misconfiguration is a human factor which cannot be eradicated completely by technology. Symptoms can be challenging to diagnose because of incorrect VLAN assignments, overlapping IP ranges, mismatched security settings then or poorly chosen quality of service parameters. These errors can be prevented from going to production through configuration audits, templated deployments and automated validation. Environmental factors like metal structures, water filled objects, reflective surfaces and thick walls affect the signal strength in various ways, depending on the physical environment. Many of these effects can be modelled by predictive design tools, but only empirical measurement can ensure that the behaviour is as predicted in the real environment.

13. OBJECTIVES OF WLAN STUDY AND DEPLOYMENT

Successful WLAN deployment starts with well stated goals. Without them, projects languish, budgets balloon, and results are less than promising. There are a few goals that are common to all industries and deployment types and should be taken into account when planning.

The first goal is to provide consistent connectivity to the desired users and devices in the desired coverage area. Reliability encompasses a number of factors, such as coverage, capacity, availability and resilience. The network which provides a signal everywhere but cannot cope with the peak loads fails on capacity. A network which operates well during normal circumstances but fails during a controller outage fails on availability. Stating reliability goals in measurable terms e.g. percentage uptime, maximum packet loss, acceptable latency provides the project team with measurable goals that they can design to.

The second goal is to safeguard the organization and its data against the wireless threats. Security goals should include protecting confidentiality of data in-transit, user and device authentication, traffic segmentation by risk, and visibility into events that may be indicative of compromise. WLAN security is a multi-layer requirement, not a single checkbox, that involves design, operation and governance.

The third goal is to enable today's and tomorrow's applications and devices. To achieve this objective it is necessary to have a detailed understanding of the application portfolio. Predictable latency is required for voice applications. For video applications, bandwidth has to be maintained. Deterministic timing is required in industrial control applications. Requirements for applications to be supported and the performance characteristics that each application needs to deliver will influence the decisions for the standards and access point density and quality of service.

The fourth is manageability. A WLAN that is deployed well, but becomes difficult to manage as time passes will deteriorate as conditions change. Manageability goals are to make it easy to monitor, troubleshoot quickly, remotely administer, and automate repetitive tasks. With the advent of cloud-managed platforms and AI-assisted operations, this goal is more attainable, but it still needs careful consideration during the procurement and design phase.

The fifth objective is to be cost-efficient throughout the whole lifecycle. Capital costs of access points and controllers are just part of the total costs. This includes cabling upgrades, switch upgrades, management licensing, operational labor and replacement costs. By setting cost goals for the entire lifecycle, the mistake of choosing the lowest cost hardware only to discover that you are spending a lot more later is avoided.

The sixth objective, which is gaining more and more recognition is sustainability. The environmental impacts of wireless infrastructure, hardware manufacturing embodied carbon and e-waste at the end of life are all issues. Organizations' commitments to sustainability and procurement choices and operational practices that reduce these impacts may also lead to cost savings.



Fig -12: Objectives of WLAN Study And Deployment

End, a strategic alignment is an objective that goes beyond the technical. The WLAN is there to serve the mission of the organization, be it to educate, treat patients, make products or serve customers. With the strategic context in mind, technical decisions are made to support business decisions and not vice versa.

14. REGULATORY AND SPECTRUM GOVERNANCE CONSIDERATIONS

Spectrum regulation has a significant impact on what WLAN operators are able to deploy, and there are significant differences in regulations from one jurisdiction to the next. The 6 GHz band, which holds a lot of the promise of Wi-Fi 6E and Wi-Fi 7, has been opened in several different ways. In the United States and Canada, the entire 1200 MHz of the 6 GHz spectrum is authorized for Wi-Fi use, which includes both low-power indoor and standard-power automated frequency coordination. The lower 500 MHz of the band have been allocated in the EU, UK, Japan and South Korea under more restrictive conditions. Some countries in the Latin American and Middle East regions have adopted the general allocation, others have adopted a conservative approach and others have yet to decide. This means that deployments across multiple countries need to support various channel plans, power limits and operating modes in a single architecture.

WLAN REGULATORY AND SPECTRUM GOVERNANCE

Different rules. Shared airwaves. A smarter, more flexible network.

Spectrum rules decide where, how and how powerful Wi-Fi can be. Plan for today, be ready for tomorrow.

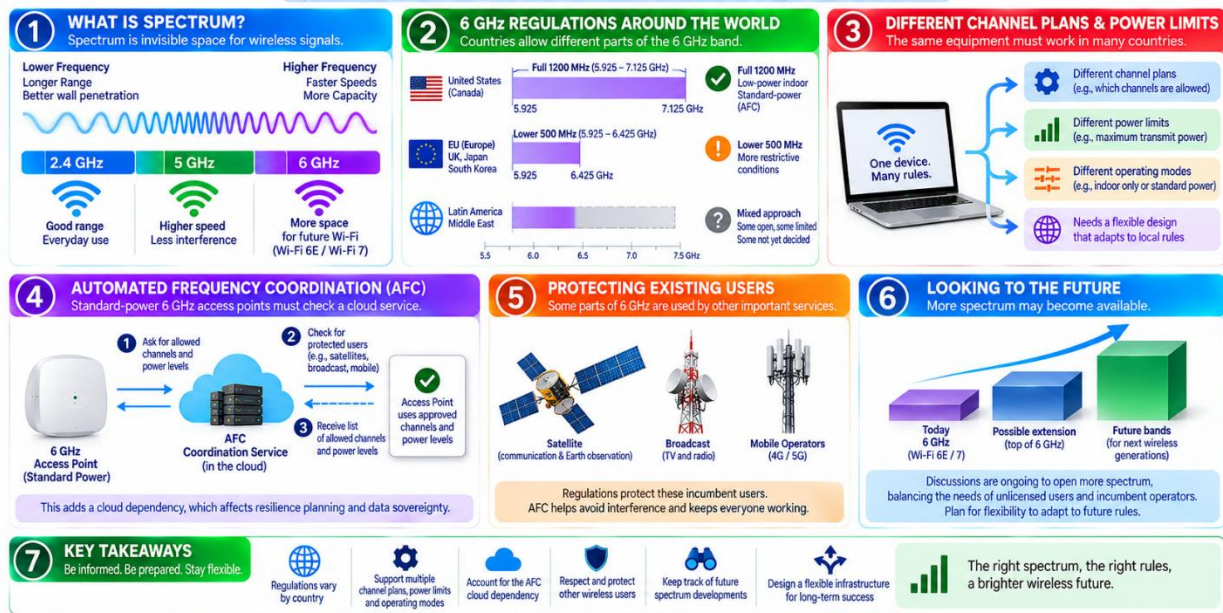


Fig -13: WLAN Regulatory And Spectrum Governance

Automated frequency coordination adds a new dependency in operation. Standard-power access points in the 6 GHz band are required to consult a coordination service that will determine the presence of protected incumbent users and provide the access point with a list of channels and power levels that are allowed for use. This means that deployments that were previously locally controlled have now introduced a cloud dependency, with ramifications for resilience planning and data sovereignty.

Looking ahead, talks are ongoing for more spectrum to be made available, such as the top of the 6 GHz band and further into the higher bands for future wireless generations. These debates are based on balancing the needs of unlicensed users with that of the incumbent satellite, broadcast and mobile operators. The results will have a significant impact on the potential of WLAN deployments in the future. Long planning organisations should keep abreast of these developments and plan for flexibility in their infrastructure options to meet changing rules.

15. CURRENT TRENDS IN 2026

The WLAN landscape in 2026 shows several trends that are merging and that altogether constitute the most important change in wireless networking since OCDMA's inception. All the trends are worth considering, for their deployment and strategy implications.

Wi-Fi 7 has gone from an emerging technology to the standard for enterprise refresh projects. Enterprise Wi-Fi access point revenue saw Wi-Fi 7 make up about fifty three percent of revenue in the second quarter of 2026, with over two hundred percent year over year revenue growth. Wi-Fi 7 accounted for approximately 44 percent of enterprise access point revenue in the first quarter, compared to less than 12 percent in the prior quarter. This transition is one of the quickest for enterprise wireless ever documented. Even if the

environment does not require the new technology, many organizations are opting for Wi-Fi 7 in multi-year refresh plans as they believe it will support them until the end of the decade.

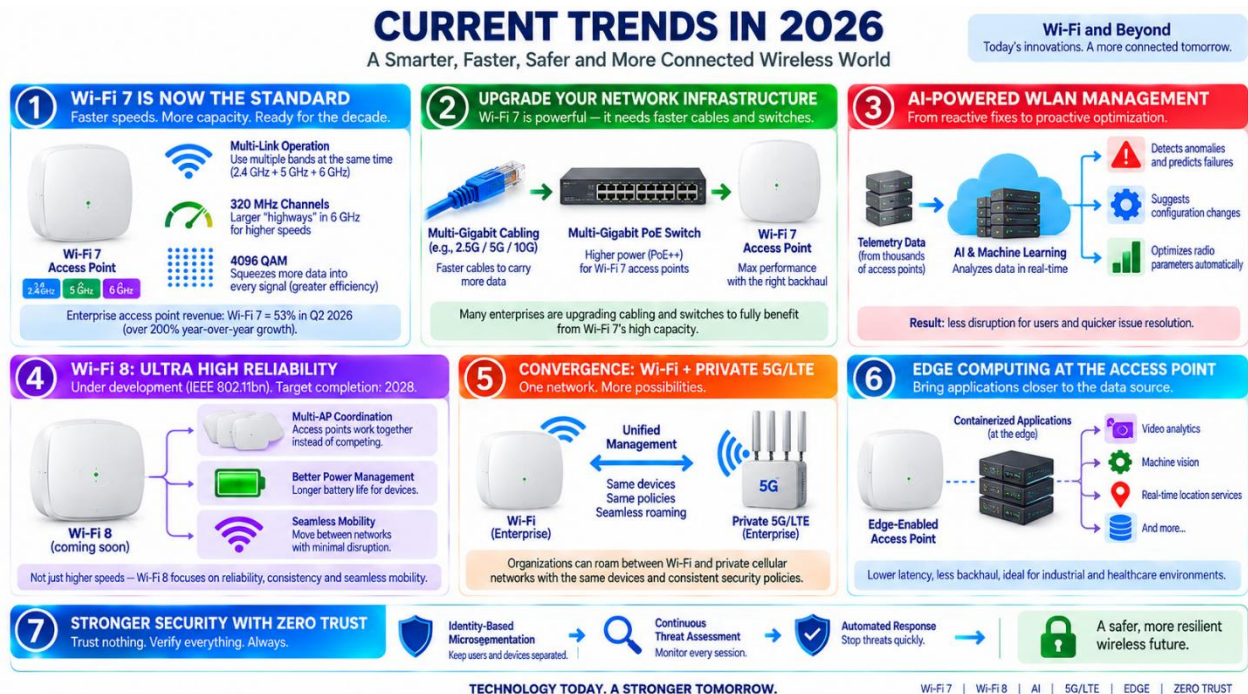


Fig -14: Current Trends in 2006

The technology that is driving Wi-Fi 7 will be multi-link operation the ability to use multiple frequency bands at once 320 MHz channel widths in the 6 GHz band for higher throughput, and 4096 quadrature amplitude modulation for greater spectral efficiency. In a real enterprise deployment, the enterprise deployment is often constrained by the capacity of one gigabit Ethernet backhaul, which is unable to support the capacity of a Wi-Fi 7 access point. Enterprises that are looking to reap the rewards of Wi-Fi 7 are investing in cabling that can handle multi-gigabit speeds, and switches that can supply the greater amount of power that these Wi-Fi 7 access points need.

One of the hallmarks of today's WLANs is the use of artificial intelligence (AI) in wireless management platforms. Telemetry data from thousands of access points is analyzed by machine learning models, which detect anomalies, forecast failures, and suggest configuration changes and optimize radio parameters in real-time. This has changed the course of operations teams from reactive troubleshooting to proactive optimization. For end users, it's meant less disruption and quicker resolution issues when they arise. Wi-Fi 8 also known as IEEE 802.11bn is currently under development and is being branded as Ultra High Reliability. The standard is expected to be completed around 2028 and initial deployments will start to emerge in the second half of 2026 reference designs. Wi-Fi 8 is not an increase in peak throughput as in the past. Rather, it's about reliability, consistency and seamless mobility. These include multi-access-point coordination, which enables cooperation between neighbouring access points, rather than competition for spectrum improved power management for battery-powered devices and seamless mobility domain, which minimises disruption when moving between networks.



Another trend that has a significant impact on enterprise wireless is the convergence of WLAN and private cellular networks. In 2026, deployments are moving towards a unified management of Wi-Fi and private LTE/5G. Roam between the technologies with the same devices and enforce consistent policies across both mediums by operations teams. In addition, integration with edge computing is making progress. At the edge of the network, access points with ample compute power host containerized applications that bring workloads closer to the data source, such as video analytics, machine vision, real-time location services, and more. This architecture helps to minimize latency and backhaul requirements, especially in industrial and healthcare environments. Last but not least, security integration is further strengthened. From design philosophy to deployment practice, zero-trust principles have gone from being trusted after initial authentication to being verified continuously for every device and session. Native support for identity-based microsegmentation, constant threat assessment and automated responses to threats detected are becoming common features of WLAN platforms.

16. FUTURE PROSPECTS AND THE TRANSFORMATION AHEAD

Beyond the current trends, there are a number of developments that will change the role of WLANs in the second half of the decade. These are not predictions but simply extensions of trends that can be seen in 2026. Applications that have been hampered by the unreliability of wireless connections will be unleashed by ultra-reliable low-latency wireless as promised by Wi-Fi 8 and beyond. Today's Wi-Fi has a hard time providing guarantees of reliability, which is essential for autonomous mobile robots in warehouses, surgical robotics in operating theaters, and real-time control systems in manufacturing. These assurances will become commonplace and the distinction between wired and wireless connectivity will fade for an ever-growing number of applications.

Another wave of demands will be for extended reality applications. For AR, VR and MR headsets, there is a need for sustained high bandwidth, low latency and consistent frame delivery. Businesses utilizing these technologies for training, design review, remote assistance and collaboration will require WLANs designed for these applications. The places that will provide top-tier wireless infrastructure for extended reality will stand out in retail, education and entertainment. Ambient IoT (Internet of Things) will increase the number of connected devices by orders of magnitude as sensors will be embedded in almost everything around us. There will be so many of these devices that will communicate infrequently and with low power, but in ways that will strain WLAN infrastructure. Under this load, features like target wake time will be crucial to allow devices to coordinate when they transmit, to keep networks manageable.

Spectrum policy will continue to develop. Regulatory agencies in several regions have recently released plans to open up the 6 GHz band to Wi-Fi, and other spectrum bands and sharing rules with incumbent users are in discussion. The results of these policy discussions will shape the future of WLAN deployments, such as whether some high density venues will be able to accommodate the bandwidth required by applications. The convergence with cellular networks will take place at a faster pace. For years, the industry has been talking about integrating Wi-Fi and cellular; 2026 is a year where there are concrete steps toward the goal of managing, authenticating and roaming between the two. In the future, enterprise networks might be a single wireless fabric to the user and the technology used to create the network would be determined automatically based on device capability, location, and policy.

Wireless design will be more impacted by sustainability. Procurement decision making will be influenced by energy efficient hardware, longer product life cycles, repairability, and proper end-of-life management.

Wireless infrastructure will have a lower environmental impact with operational practices like turning off unused access points during off hours and consolidating controllers with virtualization.



Fig -15: Future Prospects of WLANs

Last but not least, the contribution of WLAN to critical functions in society will increase. Wireless connectivity is essential for healthcare, education, public safety and emergency response. Resilient WLAN infrastructure investment, comprising of redundancy, local offline operation and interoperability with public networks will be part of wider investment to create digital resilience against disruption. The implications for organizations that are planning for this future are obvious. When making infrastructure decisions in 2026, it's important to take into account the continued increase of device density, application demand and reliability expectations. When making a procurement decision, preference should be given to platforms that can be upgraded via software and not by changing hardware. Operation practices should not be against automation and machine learning. Security postures should be based on the premise that threats will continue to evolve and that defense requires constant adaptation and is not a set configuration.

17. CONCLUSION

From convenience to critical infrastructure, wireless local area networks (WLAN) have come a long way in a generation. Initially a means of getting rid of Ethernet, what started out as a technology for freeing laptops is now used for the bulk of enterprise, residential and industrial traffic and is carrying applications that were unimaginable when it was first used. The evolution of 802.11 standards to the Wi-Fi 7 baseline of 2026 and the new Wi-Fi 8 standard with the emphasis on ultra-high reliability is a testament to an ongoing engineering journey that builds upon itself over time.

This article's analysis reveals a number of themes that have remained constant. It is important to distinguish between the terms WLAN and Wi-Fi, WLAN is a general term while Wi-Fi is a specific family of

standards. But as with any hardware, architecture is just as important, and the controllers, segmentation and policy enforcement will help make a deployment either scale gracefully or struggle. Security is a multi-layer discipline and relies on the technology and practice to work in harmony. Issues like roaming performance, dense environments and interference remain and need to be carefully designed to handle. In the future, WLANs will further develop in the direction of higher reliability, more integration into the cellular network and the edge computing, and enable applications with requirements for deterministic performance. By viewing wireless infrastructure as strategic as opposed to peripheral, organizations will be better equipped to meet the user experience, operational and adaptability needs of the connected environments that are coming.

REFERENCES

- [1] E. Khorov, I. Levitsky and I. F. Akyildiz, "Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7," in *IEEE Access*, vol. 8, pp. 88664–88688, 2020, doi: 10.1109/ACCESS.2020.2993448
- [2] Mozaffariahrar, E., Theoleyre, F., & Menth, M. (2022). A Survey of Wi-Fi 6: Technologies, Advances, and Challenges. *Future Internet*, 14(10), 293. <https://doi.org/10.3390/fi14100293>
- [3] Acalbfi.com. (2026). Wi-fi 6e technology explained: Performance, benefits & comparison with wi-fi 6 and wi-fi 7 » ACAL BFi, <https://www.acalbfi.com/news-and-insights/wi-fi-6e-technology-explained/>.
- [4] Arxiv.org. (2025). Coexistence analysis of wi-fi 6e and 5G NR-U in the 6 GHz band. <https://arxiv.org/html/2506.22844v1>.
- [5] Deng, C., Fang, X., Han, X., Wang, X., Yan, L., Rong, H., Long, Y. and Guo, Y. (2020a). IEEE 802.11be-Wi-Fi 7: New Challenges and Opportunities. *arXiv*. <https://arxiv.org/abs/2007.13401v3>.
- [6] Halbouni, A.H., Ong, L.-Y. and Leow, M.-C. (2023). Wireless security protocols WPA3: A systematic literature review. *IEEE Access*, 11, pp.1–1. doi:10.1109/access.2023.3322931.
- [7] IEEE (2018). Wireless local area networks (WLAN). *IEEE Technology Navigator*. Available at: <https://technav.ieee.org/topic/wireless-local-area-networks-wlan/>.
- [8] Kohlios, C.P. and Hayajneh, T. (2018a). A comprehensive attack flow model and security analysis for wi-fi and WPA3. *Electronics*, 7(11), p.284. doi:10.3390/electronics7110284.
- [9] Liu, X., Dong, Y., Li, Y., Lin, Y., Yang, X. and Gan, M. (2023). IEEE 802.11be wi-fi 7: Feature summary and performance evaluation. *arXiv*. <https://arxiv.org/abs/2309.15951v1>.
- [10] Metere, R., Lilli, M., Luca, A. and Riccobene, E. (2026). What a mesh: Formal security analysis of WPA3 SAE wireless authentication. *arXiv*. <https://arxiv.org/abs/2603.23352v1>.
- [11] Natkaniec, M., Prasnal, Ł. and Szymakowski, M. (2020). A performance analysis of IEEE 802.11ax networks. *International Journal of Electronics and Telecommunications*, pp.225–230. doi:10.24425/ijet.2020.131867.
- [12] Sarkar, N.I. and Gul, S. (2026). Joint effect of signal strength, bitrate, and topology on video playback delays of 802.11ax gigabit wi-fi. *Electronics*, 15(3), p.531. doi:10.3390/electronics15030531.
- [13] Seda, D.-T., Muhammad Iqbal, R., Tusha, A., Hossein, N., Helzerman, J. and Ghosh, M. (2023). Evaluating the interference potential in 6 GHz: An extensive measurement campaign of a dense indoor wi-fi 6E network. *arXiv*. <https://arxiv.org/abs/2307.00235v1>.
- [14] www.wi-fi.org. (n.d.). Wi-fi 6 and wi-fi 6E: The key to IoT | wi-fi alliance. <https://www.wi-fi.org/beacon/kevin-robinson/wi-fi-6-and-wi-fi-6e-the-key-to-iot>.
- [15] Zankiewicz, A. (2026). Practical analysis of IEEE 802.11n 2.4 GHz communication quality in the context of IoT devices operating in an area shared with modern wi-fi 6 and wi-fi 7 networks. *Sensors*, 26(17), p.5352. doi:10.3390/s26175352.
- [16] Adame, T., Carrascosa-Zamacois, M., & Bellalta, B. (2021). Time-Sensitive Networking in IEEE 802.11Be: On the way to Low-Latency WiFi 7. *Sensors*, 21(15), 4954. <https://doi.org/10.3390/s21154954>
- [17] George, D. (2026b). IEC 62443 Wireless Security: Deploying OT wireless controllers in industrial factory networks. *Zenodo* (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19428490>
- [18] Butler, B., Jirovsky, P., Anesini, D., & Cardoza, C. (2026a, June 16). Wi-Fi 7 captures 44% of enterprise WLAN dependent access point revenue as 1Q26 market grows 15.9% to nearly >.7 billion. IDC.

- <https://www.idc.com/resource-center/blog/wi-fi-7-captures-44-of-enterprise-wlan-dependent-access-point-revenue-as-1q26-market-grows-15-9-to-nearly-2-7-billion/>
- [19] George, D. (2026a). Digital dividend data taxation's potential to transform India's economy and redefine fiscal policy in the mobile era. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19021895>
- [20] Butler, B., Jirovsky, P., Anesini, D., & Cardoza, C. (2026b, September 10). Enterprise WLAN market grows 23.2% to \$3.2 billion in 2Q26, driven by accelerating Wi-Fi 7 adoption. IDC. <https://www.idc.com/resource-center/blog/enterprise-wlan-market-grows-23-2-to-3-2-billion-in-2q26-driven-by-accelerating-wi-fi-7-adoption/>
- [21] George, A. S., & George, A. (2020). A review of Wi-Fi 6: The Revolution of 6th generation Wi-Fi Technology. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.7024624>
- [22] Client challenge. (n.d.). <https://www.scribd.com/document/766228691/Wireless-Security-Protocols-WPA3-a-Systematic-Lite>
- [23] IEEE. (2025). Wi-Fi 8 key features. In Technical Deep Dive Into the 802.11bn Standard. https://www.litepoint.com/wp-content/uploads/2025/08/5_Wi-Fi_8_Key_Features_and_Goals.pdf
- [24] George, D. (2026d). Wi-Fi 8: The Shift from Speed to Reliability in Wireless Networking. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.22974325>
- [25] Kalytta, P. (2022). Automated management and performance analysis of Wi-Fi 6E (6 GHz) networks for IoT-Systems (By Prof. Dr. Andreas Grebe (Technische Hochschule Köln) & Prof. Dr. René Wörzberger (Technische Hochschule Köln)). https://www.dn.th-koeln.de/wp-content/uploads/2025/09/Kalytta-Masterarbeit_1.pdf
- [26] George, D., George, A., & Dr.T.Baskar. (2023). Wi-Fi 7: the next frontier in wireless connectivity. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.8266216>
- [27] LANCOM. (n.d.). LANCOM White Paper Wi-Fi 6E. https://rs-nc.rohde-schwarz.com/fileadmin/download/whitepaper/WP_Wi-Fi-6E_EN.pdf
- [28] George, D. (2026c). The Convergence of Intelligence and Infrastructure: A review of Emerging Technology Trends Reshaping Modern Operational Technology (OT) ecosystems. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20353281>
- [29] Qu, Q., Li, B., Yang, M., Yan, Z., Yang, A., Deng, D., & Chen, K. (2019). Survey and performance evaluation of the upcoming next generation WLANs standard – IEEE 802.11AX. *Mobile Networks and Applications*, 24(5), 1461–1474. <https://doi.org/10.1007/s11036-019-01277-9>
- [30] Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 28–35. <https://doi.org/10.32628/cseit1953127>
- [31] RUI, F. (2026, May 15). Wi-Fi 7 Enterprise deployment: What actually changes in 2026. InHand Networks. <https://inhandgo.com/blogs/solutions/wi-fi-7-enterprise-deployment-what-actually-changes-in-2026>
- [32] Sharma, D. a. K. (2026). AI-Powered Cybersecurity for OT and the IoT: A review of convergence, risk, and resilience in industrial environments. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20156818>
- [33] TP-Link Editorial Group. (2026, October 5). Wi-Fi 8 vs. Wi-Fi 7: What's the Real Difference? TP-Link. <https://www.tp-link.com/us/blog/2415/wi-fi-8-vs-wi-fi-7-what-s-the-real-difference-/>
- [34] Wheeldon, G. (2026, September 25). WiFi 7 (802.11be) explained: What changes for enterprise WiFi. Purple. <https://www.purple.ai/en-us/guides/wi-fi-7-802-11be-explained-what-changes-for-enterprise-wifi>
- [35] Wikipedia contributors. (2026a, September 8). Wi-Fi 6. Wikipedia. https://en.wikipedia.org/wiki/Wi-Fi_6
- [36] Wikipedia contributors. (2026b, October 12). Wi-Fi 8. Wikipedia. https://en.wikipedia.org/wiki/Wi-Fi_8
- [37] Wikipedia contributors. (2026c, October 12). Wi-Fi 8. Wikipedia. https://en.wikipedia.org/wiki/IEEE_802.11bn